

Security Administration Handbook

Version 8

April 27, 2010

Table of Contents

| | |
|---|-----------|
| IMPORTANT INFORMATION PLEASE READ | 6 |
| Security Administration Changes for HRMS Upgrade (Launch B)..... | 6 |
| Checklist for UserID Account Maintenance | 9 |
| SAP License Assignment Matrix | 11 |
| General Naming Conventions | 16 |
| HCM Roles | 16 |
| User Groups in HCM and BI..... | 17 |
| BI Roles | 17 |
| E-Recruiting Roles | 18 |
| Portal Roles | 18 |
| HCM AUTHORIZATION ADMINISTRATOR SR3P_XXXX_AUTH_ADMIN..... | 19 |
| Introduction..... | 20 |
| Dept. of Personnel Setup for Non-Professional UserID accounts | 20 |
| Assign Roles to Positions Using PFCG | 21 |
| Reconcile the Roles Using PFCG | 25 |
| Assign Roles to Positions Using PPOMW | 27 |
| Find the position number | 27 |
| Add the ID column..... | 29 |
| Show currently assigned roles | 29 |
| Add roles | 30 |
| Reconcile the Roles Using SU01D | 32 |
| Delete Roles from Positions Using PFCG..... | 34 |
| HCM USER ADMINISTRATOR SR3P_XXXX_USER_ADMIN | 38 |
| Maintaining a Professional HCM UserID Account | 39 |
| Enter OOSB Auth Profile..... | 39 |
| Update the UserID (SU01) | 40 |
| Single Sign On (SSO) | 42 |
| HCM UserID Maintenance | 42 |
| Reset HCM Password (SU01)..... | 42 |
| Lock/Unlock HCM UserID (SU01) | 44 |
| Mass HCM UserID Lock/Unlock (SU10) | 45 |
| Non-Professional Users (ESS Users) Leave State Employment – Employee Status is Withdrawn:..... | 48 |
| Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):..... | 48 |
| Employee has a Name Change | 50 |
| HCM SECURITY AUDITOR SR3P_XXXX_SECURITY_AUDIT | 51 |
| Display Users by Role (SUIM) | 52 |
| Display Role Assignments for all Users (SUIM)..... | 54 |
| Display Transactions by Role (SUIM) | 56 |
| Display Role Information (PFCG)..... | 57 |

| | |
|---|-----------|
| Display List of Infotypes (S_ALR_87101323) | 60 |
| Display Changes in Infotype Data (S_AHR_61016380) | 61 |
| Display User Assignments (ZAUTH_DSP_USR_ASSIGN) | 62 |
| BI (BUSINESS INTELLIGENCE) ZS_BI_XXXX_USER_ADMIN | 65 |
| Introduction..... | 66 |
| Maintaining a Professional BI UserID Account..... | 67 |
| Create BI UserID (SU01)..... | 67 |
| Single Sign On | 71 |
| Assign Professional Roles to a BI UserID Account (SU01) | 72 |
| Delete Professional Roles from a BI UserID Account (SU01) | 74 |
| BI UserID Maintenance | 75 |
| Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):..... | 75 |
| Employee has a Name Change | 76 |
| E-RECRUITING USER ADMINISTRATOR SERP_USER_ADMIN..... | 77 |
| Introduction..... | 78 |
| Types of E-Recruiting Users - New to Launch B (October 2008)..... | 79 |
| Maintaining a Professional E-Recruiting UserID Account | 80 |
| Assign Roles to E-Recruiting UserID's..... | 80 |
| Reconciling the Role | 82 |
| E-Recruiting UserID Maintenance..... | 84 |
| Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):..... | 84 |
| Employee has a Name Change | 85 |
| HRMS PORTAL – USER ADMIN | 87 |
| Introduction..... | 88 |
| Logon to the HRMS Portal | 88 |
| Professional Portal Accounts | 89 |
| Advanced Search | 90 |
| Maintaining a Professional Portal Logon ID Account | 91 |
| Creating Professional Portal Logon IDs (UME)..... | 91 |
| Assigning Group Roles to Professional LDAP or UME LogonID's..... | 94 |
| Assigning User Admin Single Role to Professional LDAP or UME LogonID's | 96 |
| Mapping to BI UserID | 97 |
| Portal LogonID Maintenance..... | 98 |
| Reset Portal Logon ID Password | 98 |
| Lock/Unlock Portal Logon ID's | 99 |
| To LOCK a specific Portal Logon ID | 99 |
| To UNLOCK a specific Portal Logon ID | 101 |
| Delete PORTAL domain\username Accounts (UME) | 102 |
| Delete Access from PORTAL E-Mail Account (LDAP) | 105 |
| Non-Professional Users (ESS Users) Leave State Employment – Employee Status is Withdrawn:..... | 107 |

| | |
|---|-----|
| Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):..... | 108 |
| Employee has a Name Change | 112 |
| Changing the Name in the ESS or domain\username (UME) Portal Account | 112 |
| Changing the LogonID for the domain\username (UME) Portal Account | 113 |

Important Information Please Read

Security Administration Changes for HRMS Upgrade (Launch B)

Launch B provides new functionality for E-Recruiting and Grievance Professional Users:

- ❖ E-Recruiting through the HRMS Portal (Available 11/22/08)
- ❖ Some E-Recruiting and Grievance reports available through the HRMS Portal BI_Reports tab (Coming Soon)

Users who want to take advantage of this new functionality may need additional accounts and new roles in the HRMS Portal and in Business Intelligence (BI).

Below is a summary of the UserID accounts and setup needed to access this new functionality. For specific details on how to set up each user, please refer to the appropriate sections of this handbook. Agency Security Administrators must complete these steps.

E-RECRUITING USER – Access via the Portal - NO authorization for BI Reports

| CLIENT | USERID ACCOUNT | ROLES (One or More) |
|------------------------|--|--|
| EPO | 8-digit Pernr account | SERP_RCF_ASSESSMENT SERP_RCF_DE_ADMIN_LIMITED SERP_DE_RCF_JOB_SEEKER_SUPPORT SERP_RCF_DECISION_MAKER SERP_RCF_MGR_AS_RECRUITER SERP_RCF_RECRUITER SERP_RCF_RECRUITER_LIMITED SERP_RCF_RECRUITER_SUPPORT SERP_RCF_REQ_REQUESTER |
| BIP | 8-digit Pernr account Note: may have other BI roles for HR/FI/GR/ER | ZS_BI_GENERAL_ACCESS |
| HRMS PORTAL | Professional UserID - There are two different types: LDAP UserID: This account already exists in the portal. Users that are part of the state's Active Directory tree access the portal with their email address and network password. UME UserID: Agency Portal User Administrators create this account. The format for UME accounts are: agency domain\username (for example dop\mickeym). | ER_Assessment_GRP ER_DecentralAdminLimited_GRP ER_DeCentralJSSupport_GRP ER_DecisionMaker_GRP ER_ManagerAsRecruiter_GRP ER_Recruiter_GRP ER_RecruiterLimited_GRP ER_RecruiterSupport_GRP ER_RequisitionRequest_GRP |
| | Map the Professional User account to their BIP Pernr UserID | |

E-RECRUITING USER – Access via the Portal - Authorization for BI Reports

| CLIENT | USERID ACCOUNT | ROLES (One or More) |
|------------------------|--|---|
| EP0 | 8-digit Pernr account | SERP_DE_REPORTS_AGYWIDE or SERP_DE_REPORTS_DIVERSITY or SERP_DE_REPORTS_LTD or |
| BIP | 8-digit Pernr account | ZS_BI_XXXX_END_USER and (XXXX is 4 or 5 digit agency number) ZS_BI_XXXX_WBWT and ZS_BI_SOW_WBWT and ZS_BI_GENERAL_ACCESS and ZS_BI-ER_ANALYSIS (Infocube role) |
| | Notes: If this is an existing BI User who has a POWER_USER or END_USER role, you only need to add the ZS_BI-ER_ANALYSIS role. Depending on other requirements, the user may also have FI and/or HR and/or GR Analysis roles. Centralized E-Recruiting roles are handled by DOP. | |
| HRMS PORTAL | Professional UserID - LDAP or UME | BI_REPORTS_GRP |
| | Map the Professional User account to their BIP Pernr UserID | |

GRIEVANCE USER – Access via the Portal - Authorization for BI Reports

| CLIENT | USER ACCOUNT | ROLES |
|------------------------|---|---|
| RP0 | 8-digit Pernr account | SR3P_DE_GRIEVANCE_ADMIN or SR3P_DE_GRIEVANCE_INQ |
| BIP | 8-digit Pernr account | ZS_BI_XXXX_END_USER (XXXX is 4 or 5 digit agency number) ZS_BI_XXXX_WBWT ZS_BI_SOW_WBWT ZS_BI_GENERAL_ACCESS ZS_BI-GR_ANALYSIS (Infocube role) |
| | Notes: If this is an existing BI User who has a POWER_USER or END_USER role, you only need to add the ZS_BI-GR_ANALYSIS role. Depending on other requirements, the user may also have FI and/or HR and/or ER Analysis roles. Centralized Grievance roles are handled by DOP. | |
| HRMS PORTAL | Professional UserID – LDAP or UME | BI_REPORTS_GRP |
| | Map the Professional User account to their BIP Pernr UserID | |

DECENTRALIZED SECURITY ADMINISTRATORS

| CLIENT | USER ACCOUNT | ROLES |
|------------------------|--|---|
| RP0 | 8-digit Pernr account Add entry in the OOSB (T77UA) with the appropriate authorization data profile | SR3P_XXXX_USER_ADMIN and/or SR3P_XXXX_AUTH_ADMIN |
| BIP | 8-digit Pernr account | ZS_BI_XXXX_USER_ADMIN ZS_BI_GENERAL_ACCESS |
| EP0 | 8-digit Pernr account | SERP_USER_ADMIN |
| HRMS PORTAL | Professional UserID – LDAP or UME | User Admin Role on the Assigned Roles tab |

Checklist for UserID Account Maintenance

This checklist outlines what is required in each of the systems in order for a professional user to have appropriate access in the Human Resource Management System. This also outlines the steps to complete on professional and non-professional user accounts when employees transfer to other agencies or are withdrawn from state employment.

I. HCM Professional Users

- Roles assigned to the position in HCM
- SU01 User Account with validity dates and Agency User Group
- >For SSO Users ONLY: Entry in SNC tab
- Note: Effective April 27, 2010 agency Security Administrators will no longer need to assign licenses in SU01. Licenses are now assigned automatically to the user account based on the roles assigned.
 - Entry of Authorized Profile in OOSB
 - If PERS_ADMIN_PROC role is assigned add additional entry of WA_SOW in OOSB

II. BI Professional Users

- Roles assigned in BI
- SU01 User Account with validity dates and Agency User Group
- >For SSO Users ONLY: Entry in SNC tab
- Entry of Authorized Profile in OOSB in HCM
- Note: Effective April 27, 2010 agency Security Administrators will no longer need to assign licenses in SU01. Licenses are now assigned automatically to the user account based on the roles assigned.*

III. E-Recruiting Professional Users

- Role(s) assigned in E-Recruiting
- Note: Effective April 27, 2010 agency Security Administrators will no longer need to assign licenses in SU01. Licenses are now assigned automatically to the user account based on the roles assigned.*

IV. Portal Professional Users

- Email address (LDAP) or agency domain\username (UME) UserID account
- BI Reporting for E-Recruiting, Grievance, HR or Finance :
 - SU01 User Account with validity dates (HCM – Section I)
 - Entry of Authorized Profile in OOSB (HCM –Section I)
 - SU01 User account with role(s) and validity dates in BI (BI - Section II)
 - BI_Reports_GRP role assigned to the Professional portal account
 - Professional Portal account mapped to user's BI account
 - **Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapped to the Federated Portal.*
- E-Recruiting Functionality (*Professional Users in EP0*):
 - Role(s) assigned in E-Recruiting (E-Recruiting - Section III)
 - SU01 User account with General_Access role and validity dates in BI (BI - Section II)
 - Assign E-Recruiting Group role(s) that match E-Recruiting role(s) in Portal
 - Portal account mapped to user's BI account
 - **Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapped to the Federated Portal.*
- WEBGUI users
 - Roles assigned to the position in HCM (HCM – Section I)
 - SU01 User account with General_Access role and validity dates in BI (BI - Section II)
 - HR_HTMLGUI_GRP role assigned to the Professional portal account
 - Professional Portal account mapped to user's BI account
 - **Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapped to the Federated Portal.*

When Employees Transfer out of the Agency (Professional Users Only)

- HCM – Delete employees profile entries in OOSB
 - HCM – Change the User Group back to ESSUSER in SU01
 -
 - HCM – Delete the SNC entry – SSO only
 - BI – Delete the BI user account
 - E-Recruiting – Delete roles ONLY
 - Portal – Delete user mapping for agency Domain\Username – UME Professional account
 - Portal – Delete the Professional account (agency Domain\Username - UME) - LDAP e-mail address account cannot be deleted
 - Portal – Delete the Group and/or User_Admin roles (LDAP)
 - Portal – Delete user mapping for e-mail address account (LDAP)
- **Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal.***

When Employees Leave State Employment – Withdrawn Status (Professional and Non-Professional Users)

- HCM – Delete profile entries in OOSB if there are entries
 - HCM – Delete the user account (SU01) – this takes away user's access to ESS
 - BI – Delete the BI user account if created
 - E-Recruiting – Delete roles ONLY
 - Portal – Delete the ESS account (8 digit personnel number - UME)
 - Portal – Delete user mapping for agency Domain\Username – UME Professional account
- **Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal.***
- Portal – Delete the Professional account (agency Domain\Username - UME) LDAP e-mail address account cannot be deleted
 - Portal – Delete the Group and/or User_Admin roles from the e-mail address account (LDAP)
 - Portal – Delete user mapping for e-mail address account (LDAP)
- **Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal.***

SAP License Assignment Matrix

Note: Effective April 27, 2010 agency Security Administrators will no longer need to assign licenses in SU01. Licenses are now assigned automatically to the user account based on the roles assigned. License information will no longer show in SU01, in the LicenceData Tab. This matrix is for reference only. If you have questions about licenses please contact the DOP Service Center at 360-664-6400 or servicecenter@dop.wa.gov.

HCM (RP0)

| Column A | Column B | Column C |
|---|--|-------------------------------|
| mySAP Business Suite Professional | mySAP Business Suite Limited Professional | mySAP Business Suite Employee |
| SR3P_XXXX_AUTH_ADMIN SR3P_XXXX_USER_ADMIN SR3P_CE_GRIEVANCE_ADMIN SR3P_CE_OST_PAYOPS_ADMIN SR3P_CE_SECURITY_AUDIT SR3P_DE_BENE_PROC SR3P_DE_GARNISH_ADMIN SR3P_DE_GRIEVANCE_ADMIN SR3P_DE_FIN_RPT_PROC SR3P_DE_LEAVE_CORR_PROC SR3P_DE_ORG_MANG_PROC SR3P_DE_PAY_ANL SR3P_DE_PAY_PROC SR3P_DE_PAY_SUPV SR3P_DE_PERS_ADMIN_PROC SR3P_DE_PERS_ADMIN_SUPV SR3P_DE_QUALADM SR3P_DE_T&A_PROC SR3P_DE_T&A_SUPV and SR3P_SOW_ESSUSER | SR3P_XXXX_DATA_PROFILE SR3P_XXXX_SECURITY_AUDIT CR3P_CE_INQ_HELP_DESK SR3P_CE_BENEFITS_INQ SR3P_CE_GARN_INQ SR3P_DE_GRIEVANCE_INQ SR3P_DE_ORG_MGT_INQ SR3P_DE_PAY_INQ SR3P_DE_PERS_ADMIN_INQ SR3P_DE_T&A_INQ and SR3P_SOW_ESSUSER | SR3P_SOW_ESSUSER |

Business Intelligence (BIP)

| Column A | Column B |
|--|--|
| mySAP Business Suite Professional | mySAP Business Suite Limited Professional |
| ZS_BI_XXXX_USER_ADMIN ZS_BI_XXXX_POWER_USER | ZS_BI_XXXX_END_USER ZS_BI_XXXX_SECURITY_AUDIT ZS_BI_XXXX_WBWT ZS_BI_GENERAL_ACCESS ZS_BI_SOW_WBWT ZS_BI-ER_ANALYSIS ZS_BI-FI_ANALYSIS ZS_BI-FI_SOW_ANALYSIS ZS_BI-GR_ANALYSIS ZS_BI-GR_SOW_ANALYSIS ZS_BI-HR_ANALYSIS ZS_BI-HR_SOW_ANALYSIS |

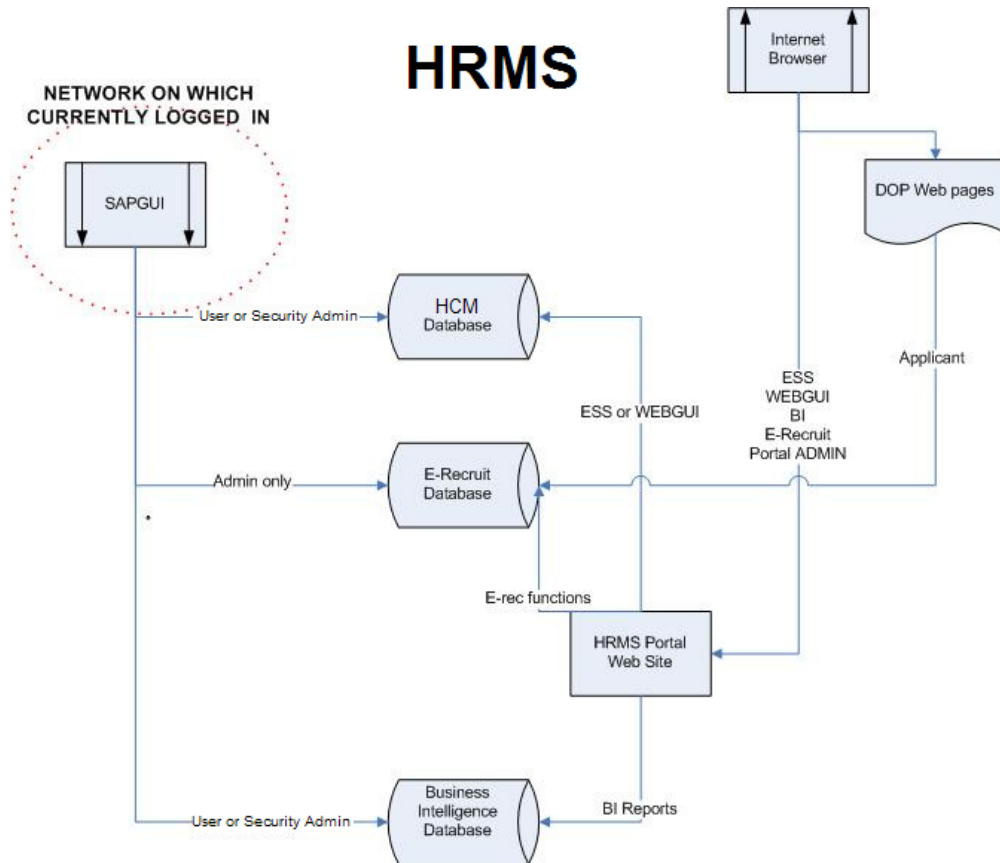
E-Recruiting (EP0)

| Column A | Column B | Column C |
|---|--|---|
| mySAP Business Suite Professional | mySAP Business Suite Limited Professional | License field is blank |
| SERP_CE_RCF_BUSINESS_ADMIN SERP_CE_RCF_JOB_SEEKER_SUPPORT SERP_CE_RCF_RECRUITER SERP_CE_RCF_USERLIST_ADMIN SERP_CE_SYSADM_RPTS SERP_DE_RCF_BUSINESS_ADMIN SERP_DE_RCF_JOB_SEEKER_SUPPORT SERP_RCF_ASSESSMENT SERP_RCF_DE_ADMIN_LIMITED SERP_RCF_MGR_AS_RECRUITER SERP_RCF_RECRUITER SERP_RCF_RECRUITER_LIMITED SERP_RCF_RECRUITER_SUPPORT SERP_RCF_REQ_REQUESTER SERP_RCF_RESTRICTED_RECRUITER SERP_USER_ADMIN SERP_WFM_DEVELOPER_LIMITED | SERP_CE_COMPLIANCE_ADMIN SERP_CE_REPORTS SERP_CE_REPORTS_DIVERSITY SERP_DE_REPORTS_AGYWIDE SERP_DE_REPORTS_DIVERSITY SERP_DE_REPORTS_LTD SERP_RCF_COMPLIANCE_ADMIN SERP_RCF_HIRE_MGR_SURVEY SERP_RCF_REQUISITION_OWNER | No Roles are Assigned, mySAP Business Suite Employee license will be automatically inherited from the RCF_CAND_INT reference user. |

Systems Overview

As a Human Resource Management System (HRMS) Security User or Authorization Administrator, you will be responsible for assisting your agency professional staff interface with the DOP HRMS. HRMS consists of: Human Capital Management (HCM), E-Recruiting, Business Intelligence (BI) and Enterprise Portal (HRMS Portal)

The chart below describes all of the systems and how they are accessed in very general terms:



The "SAPGUI" noted at the top left of the diagram is a Desktop application entry point. If your agency works within the State Government Network (SGN), the SAPGUI gives you a "stateful" connection to the following applications:

- HCM database of Personnel and Payroll information
- E-Recruiting Database
- Business Intelligence (BI) - previously called "Business Warehouse"

If you are in a K-20 system or the Military system or otherwise OUTSIDE the SGN, specific arrangements can be made with DOP or DIS in order for your agency to access the HRMS systems.

The HRMS Portal is an alternative method of entering the various systems using a professional portal UserID (LDAP or agency UME).

The HRMS Portal is the ONLY way to enter Employee Self Service (ESS) using an 8 digit pernr.

The HRMS Portal is available for access from outside the SGN via the internet -

<https://wahrms.wa.gov/iri/portal>

The HRMS Portal is available for access from inside the SGN via the internet -

<https://myhrms.wa.gov/iri/portal>

General Naming Conventions

There are several parts/nodes to the role names in the HRMS. The following is the explanation of each node:

- The First Node identifies whether the role is a “**S**”ingle role or “**C**”omposite, “**R3**” or “**ER**” and that it is a “**P**”roduction role
 - Single roles will begin with “**S**”
 - Composite roles (roles made up of single roles) will begin with “**C**”
 - HCM (old R3) Roles will have “**R3**” as the second and third characters in the role name.
 - ER Roles will have “**ER**” as the second and third characters in the role name.
 - The fourth character will be “**P**” identifying the role as a production role.
- The Second Node identifies whether the role is (“**DE**”centralized or “**CE**”ntralized) or custom
 - Decentralized roles and “SR3P_SOW_ESSUSER” may be assigned by agency Authorization Administrators.
 - Centralized and custom roles may only be assigned by DOP.
- All subsequent Nodes describe the intended role function.
 - Example: SR3P_DE_PAY_ANL – Decentralized Payroll Analyst, built as single role and assignable by agencies.
- BI roles begin with ‘ZS_BI*’ the remaining characters being as descriptive as possible to match the role name.
 - Example: ZS_BI_1110_USER_ADMIN – BI User Administrator for a particular agency.

HCM Roles

HCM Roles generally consist of at least one Decentralized Role or Centralized Role and a Structural Data Profile Role.

Security Admin, Auth and Audit Roles consist of at least one Security/Auth/Audit Role and a Structural Data Profile Role.

- Decentralized HR Roles begin with ‘SR3P_DE*’ with the remaining characters being as descriptive as possible to match the role name.
 - Example: SR3P_DE_PAY_ANL – Decentralized Payroll Analyst
- Centralized HR Roles begin with ‘SR3P_CE*’ with the remaining characters being as descriptive as possible to match the role name.
 - Example: SR3P_CE_FINC_APRV – Centralized Financial Approver
- Security Admin and Auth Roles begin with ‘SR3P_XXXX*’ with the remaining characters being as descriptive as possible to match the role name, and XXXX being the Personnel Area/Agency.
 - Example: SR3P_1110_AUTH_ADMIN – DOP Authorization Administrator
- Structural Data Profile Roles begin with ‘SR3P_XXXX_DATA_PROFILE’ with XXXX being the Personnel Area/Agency.
 - Example: SR3P_1110_DATA_PROFILE – DOP Structural Profile Role
- Security Audit Roles consist of Decentralized SR3P_XXXX_SECURITY_AUDIT or SR3P_CE_SECURITY_AUDIT.

NOTE: All Centralized roles are assigned by DOP.

User Groups in HCM and BI

- User Groups are formatted as follows: WA_XXXX
 - Where XXXX = Personnel Area/Agency
- The description should match the agency name (example follows)
 - User Group: WA_1110
 - Description: Department of Personnel

BI Roles

BI professional users are required to have an HCM UserID with an agency Data Profile Role assigned to their position and the agency authorization profile entered in the OOSB, before creating the BI UserID account.

BI Roles Include:

- one End or Power User role – ZS_BI_XXXX_POWER_USER / ZS_BI_XXXX_END_USER
 - one or more of the InfoCube Roles – ZS_BI-FI_ANALYSIS, ZS_BI-HR_ANALYSIS, ZS_BI-ER_ANALYSIS, ZS_BI-GR_ANALYSIS
 - agency and statewide Workbook/Web Template Roles – ZS_BI_XXXX_WBWT and ZS_BI_SOW_WBWT
 - the General Access role – ZS_BI_GENERAL_ACCESS
- BI End User, Power User, and Workbook/Web Template Roles begin with 'ZS_BI_*' and Personnel area with the remaining characters being as descriptive as possible to match the role name.
 - Example: ZS_BI_1110_END_USER – DOP BI End User
 - BI InfoCube Roles (HR, FI, ER, or GR) begin with 'ZS_BI_-' with the remaining characters being as descriptive as possible to match the role name.
 - Example: ZS_BI-FI_ANALYSIS
ZS_BI-FI_SOW_ANALYSIS
ZS_BI-HR_ANALYSIS
ZS_BI-HR_SOW_ANALYSIS
ZS_BI-ER_ANALYSIS
ZS_BI-GR_ANALYSIS
ZS_BI-GR_SOW_ANALYSIS
 - Security Admin Roles begin with 'ZS_BI_XXXX*' with the remaining characters being as descriptive as possible to match the role name, and XXXX being the Personnel Area/Agency.
 - Example: ZS_BI_1110_USER_ADMIN – DOP UserID Administrator for BI

E-Recruiting Roles

- Decentralized E-Recruiting Roles begin with 'SERP_DE*' with the remaining characters being as descriptive as possible to match the role name.
 - Example: SERP_DE_REPORTS_AGYWIDE
- Centralized E-Recruiting Roles begin with 'SERP_CE*' with the remaining characters being as descriptive as possible to match the role name.
 - Example: SERP_CE_RCF_RECRUITER
- Security User Admin role in E-Recruiting does not distinguish between personnel areas. The role is SERP_USER_ADMIN

Portal Roles

Portal Roles include:

- Portal User Admin – Single role
- BI_Reports_GRP – Group role – Accessing BI Reports through the HRMS Portal.
- HR_HtmlGui_GRP – Group role – Accessing HRMS through the HRMS Portal
- ESS_GRP – Group role – Accessing Employee Self Service
- Various ER_* Group Roles to access E-Recruiting functionality through the HRMS Portal. These roles should match the roles that are assigned to the Professional E-Recruiting users in EP0. See the HRMS Portal section of the Handbook.

HCM Authorization Administrator SR3P_XXXX_AUTH_ADMIN

Introduction

Security within the HRMS is based on a record called a “UserID”. A UserID is necessary to enter a specific system within the HRMS. It is distinct and separate from personnel records and is the primary responsibility of the UserID Administrator. Things like name changes in the personnel/payroll records do NOT propagate to the UserID records.

Each UserID may be assigned Professional Roles which define how the user will interface with the specific system within the HRMS. In the Personnel/Payroll system (aka HRMS, R3 or HCM)

Professional roles are divided into the following areas:

- Personnel
- Payroll
- Time & Attendance
- Grievance
- Organizational Management
- Security Administration

In each of those functional areas, there are tiers of access:

- “Processor” or “Administrator” levels have the most authority to update Master Data;
- “Inquiry” roles, which can view Master Data, cannot update it.
- “Supervisor” roles have some qualities of both Processors and Inquirers.

There are other roles available in the system, but decentralized agency authorization administrators only have the authority to assign roles available to their agencies.

Dept. of Personnel Setup for Non-Professional UserID accounts

1. DOP creates UserID for new hires (SU01)
2. DOP links Personnel Record to UserID (PA30)
3. DOP assigns the SR3P_SOW_ESSUSER role
4. DOP creates ESS Portal accounts for new employees
5. DOP distributes ESS passwords to User Administrators

NOTE:

- New employee UserIDs are created by DOP twice weekly. DOP creates Employee Self Service UserIDs (Pernr-based) in the Portal. These ESS Portal accounts have access to ‘My Personal Information’, ‘My Earnings Statement’ and ‘My Career’ where the user can create their internal E-Recruiting profile and apply for state jobs.


Assign Roles to Positions Using PFCG

Prerequisites:

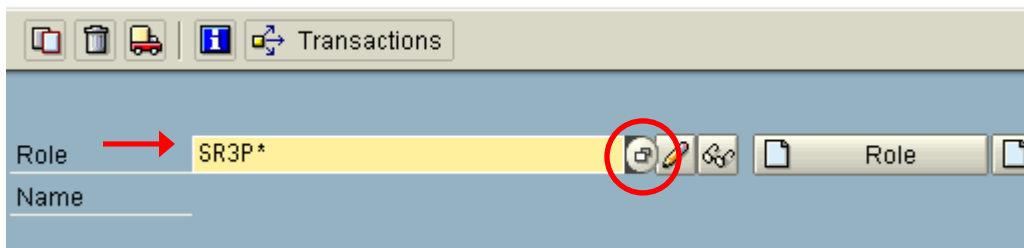
- ✓ Role name(s)
- ✓ SAP position number(s).


NOTE: To quickly find the position number, do the following:

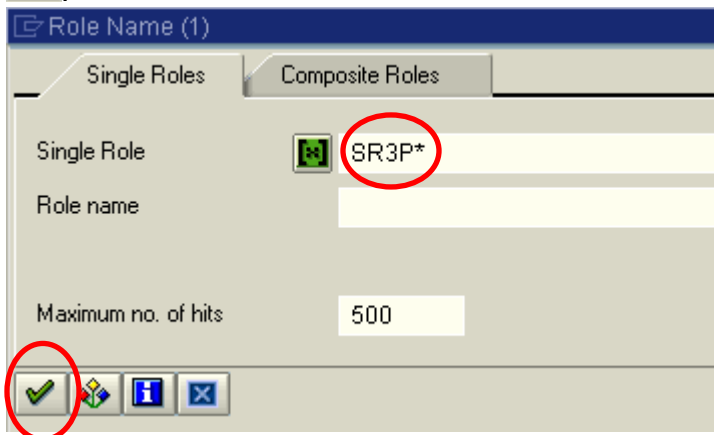
PA20 → Enter Personnel number → Select Actions → Display → the position number will be under Organizational Assignment block in the middle of the screen. Copy the position number and continue with the Role Assignment steps below.

1. Enter transaction '**PFCG**' (/nPFCG) to assign roles to positions.
2. If you know the fully qualified role name, enter it in the 'Role' field, and skip to Step 5. Otherwise, search for a role that needs to be assigned to a position. Key SR3P* (for single role) or CR3P* (for composite role) and click on .

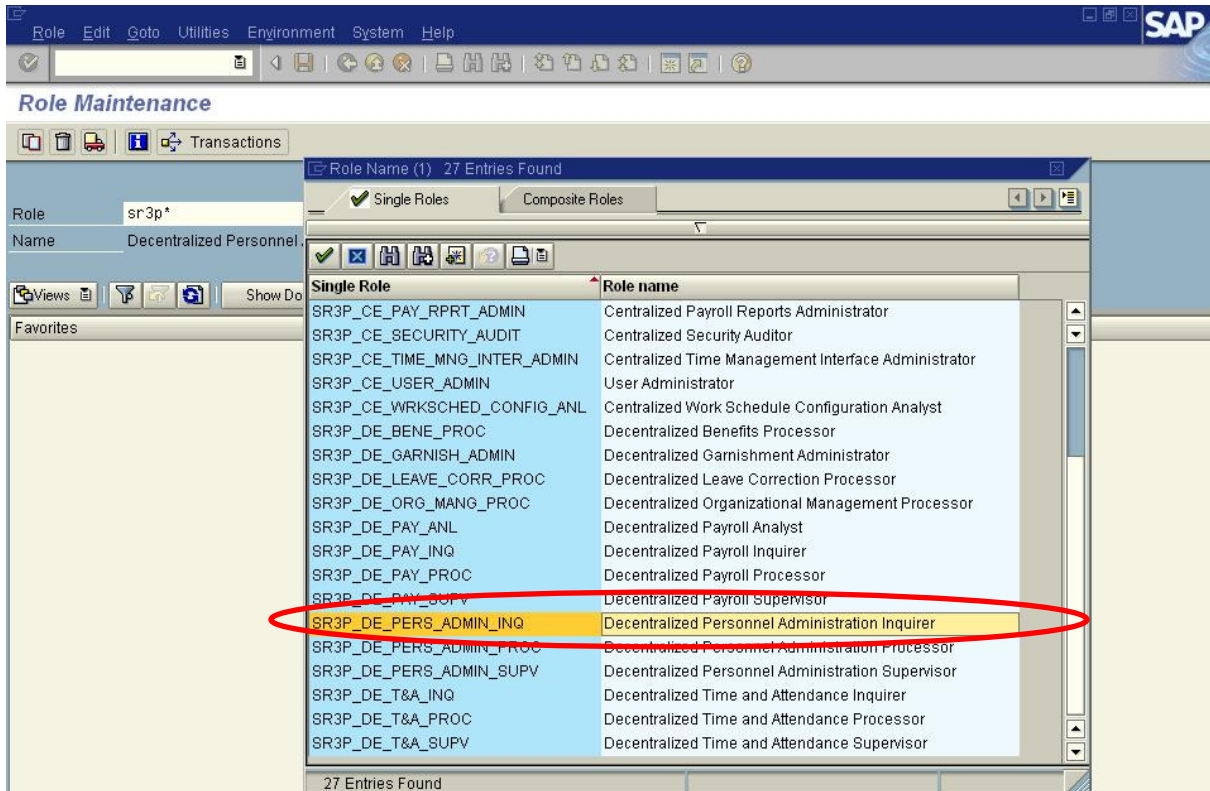
Role Maintenance




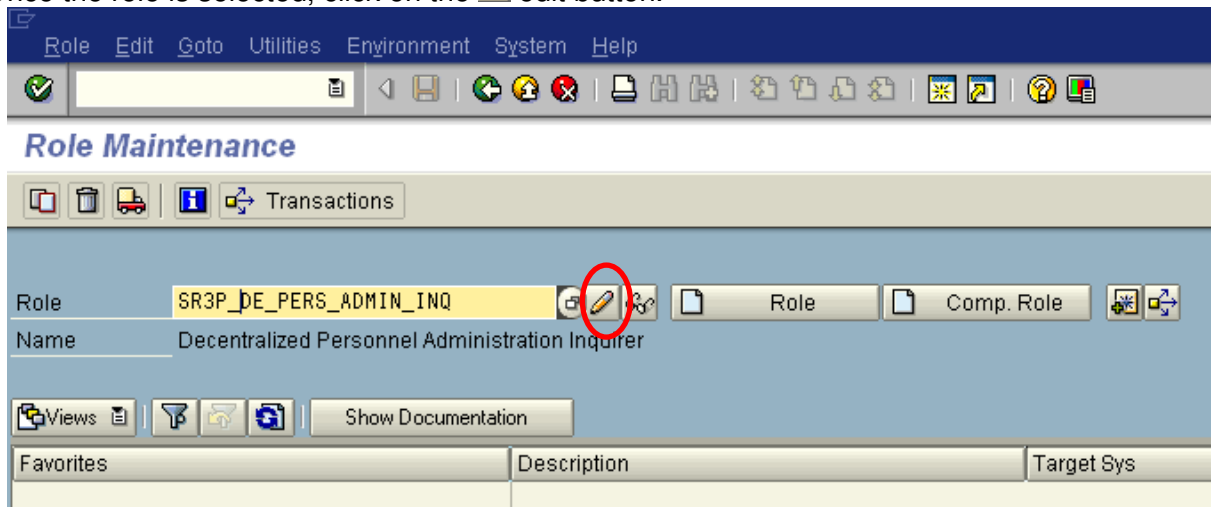
3. Verify/confirm the proper tab ('Single Roles' for SR3P*; 'Composite Roles' for CR3P*) and click on .




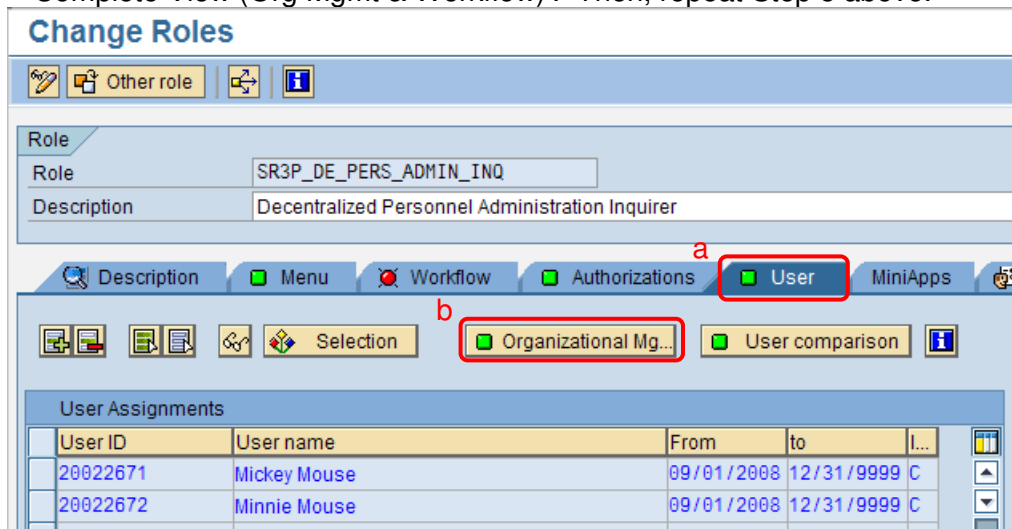
4. Double click on the appropriate role; for this example, 'Personnel Administration Inquirer' is selected.



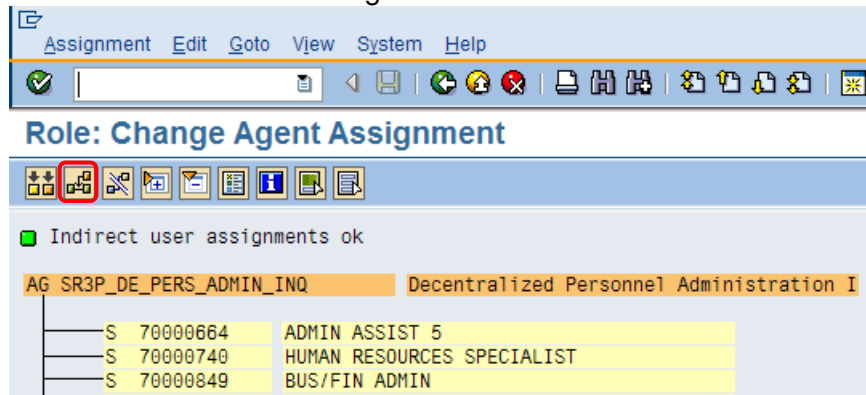
5. Once the role is selected, click on the  edit button.




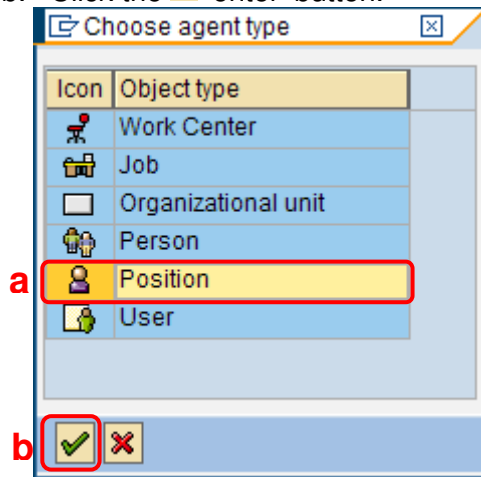
- a. Click on the 'User' tab
- b. Click on the "Organizational Mg..." button. **IF this button does not appear**, click on the  'back' button, then click 'Goto' pull-down menu (on menu bar), select 'Settings' and select 'Complete View (Org Mgmt & Workflow)'. Then, repeat Step 5 above.




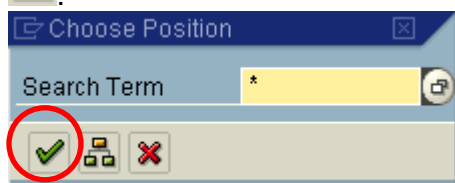
6. Click on the  'Create Assignment' button.




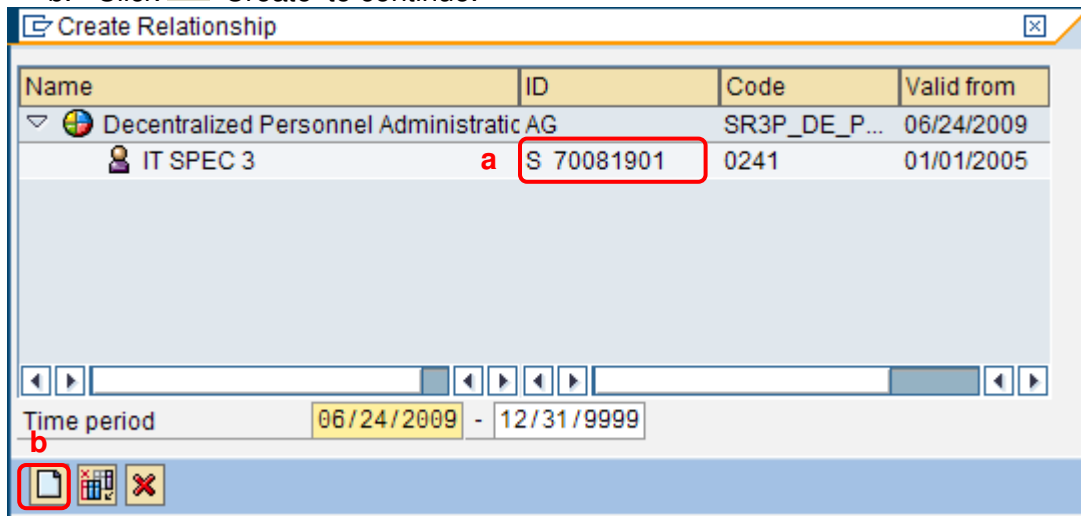
7. Choose agent type
 - a. Click on 'Position' as the object type
 - b. Click the  'enter' button.



8. Enter SAP position number (w/o the 'S') in 'Search Term' field (overlay/replace the *), and click on .






9. The appropriate role and position should be displayed.
 - a. Confirm/verify SAP Position number is correct.
 - b. Click  'Create' to continue.













Reconcile the Roles Using PFCG

10. The position should now be displayed.

- Click on the  to drill down within the position to make sure that it contains the correct person and the UserID.
- Notice that there is a red button  at the top of the screen.
- Click on  'Indirect user assignment reconciliation' button and the button should then turn green



Role: Change Agent Assignment

c         


b  Require reconciliation of indirect user assignment

AG SR3P_DE_PERS_ADMIN_INQ Decentralized Personnel Administration I










| | | |
|----|----------|----------------------------|
| S | 70000664 | ADMIN ASSIST 5 |
| S | 70000740 | HUMAN RESOURCES SPECIALIST |
| S | 70000849 | BUS/FIN ADMIN |
| S | 70081901 | IT SPEC 3 |
| P | 20022668 | Bell Tinker R |
| US | 20022661 | Tinker Bell |
| S | 70081966 | HUM RES CNSLT 3 |
| S | 70082049 | CONF SEC - WSP |

a  










- Upon successful update you will see the following message in the status area:


 Data has been saved

- Once the button is green, back out of this screen.

Role: Change Agent Assignment





        

 Indirect user assignments ok

11. The UserID and user name should now be included in the list, in blue.







NOTE: Blue means the employee has roles assigned by position. You should always assign roles to position and not directly to the UserID.

Change Roles



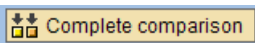
Role
Role: SR3P_DE_PERS_ADMIN_INQ
Description: Decentralized Personnel Administration Inquirer

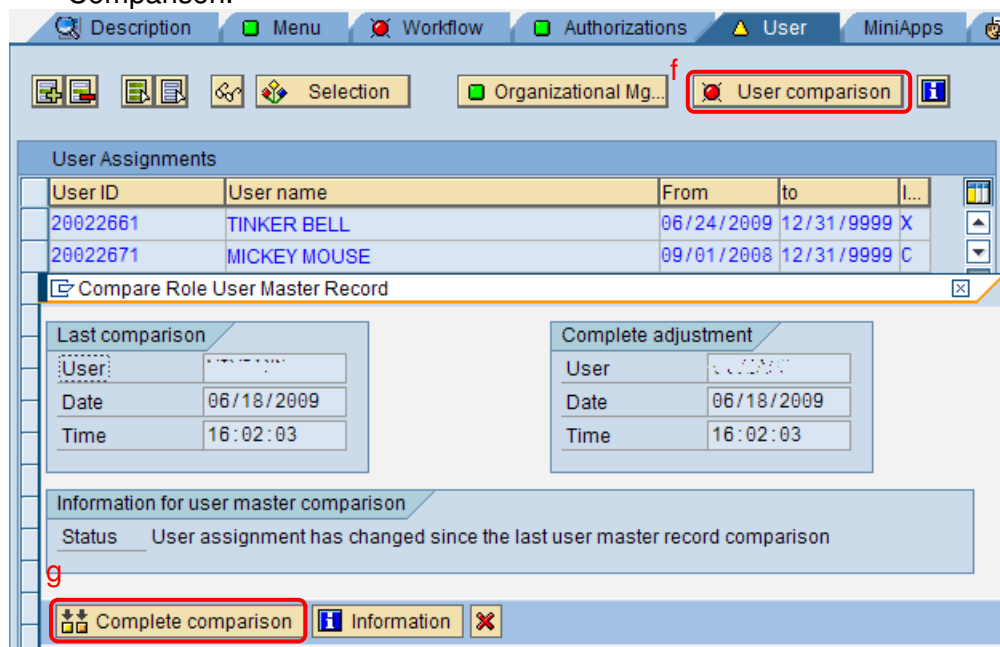
Description Menu Workflow Authorizations User MiniApps

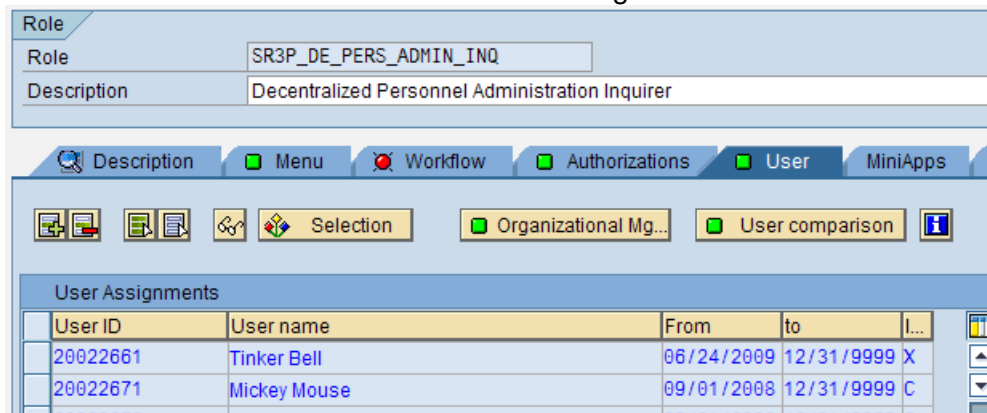
User Assignments


| User ID | User name | From | to | I... |
|----------|--------------|------------|------------|------|
| 20022661 | Tinker Bell | 06/24/2009 | 12/31/9999 | X |
| 20022671 | Mickey Mouse | 09/01/2008 | 12/31/9999 | C |
| 20022672 | Minnie Mouse | 09/01/2008 | 12/31/9999 | C |

12. If the  'User comparison' button is red,
- Click on the  button
 - In the Compare Role User Master Record popup, click on  'Complete Comparison.'



13. All buttons within the 'User' tab should now be green.



14. Click the 'Save'  button to save changes to the role.
15. Follow the same steps for [Assign Roles to Positions \(PFCG\)](#) to assign the agency Data Profile role with the following naming convention: SR3P_XXXX_DATA_PROFILE – where XXXX is your Personnel Area.
16. Contact your User Administrator after all roles are assigned, they need to go to SU01 and [complete the steps for maintaining a professional user](#).

Assign Roles to Positions Using PPOMW

NOTE: PPOMW transaction lets you assign multiple roles at once.

Prerequisites:


- ✓ User's name or
- ✓ Users UserID/Personnel Number (8 digits) or
- ✓ SAP Position number

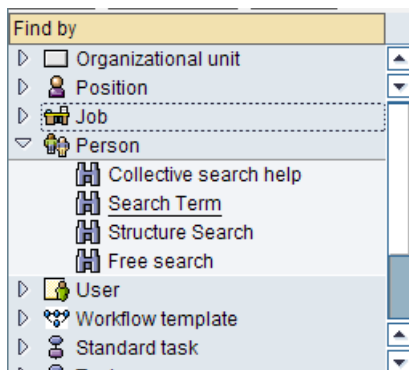
NOTE: You must always assign roles to positions.

1. Enter transaction '**PPOMW**' (/nPPOMW). You will see in the status area. Disregard this message and continue.

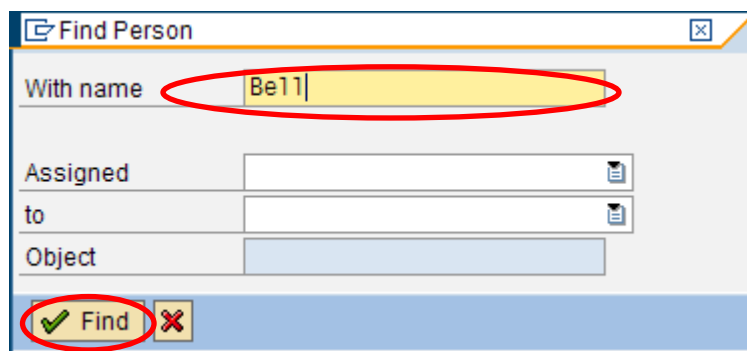
✓ You have no authorization to change or delete.

Find the position number

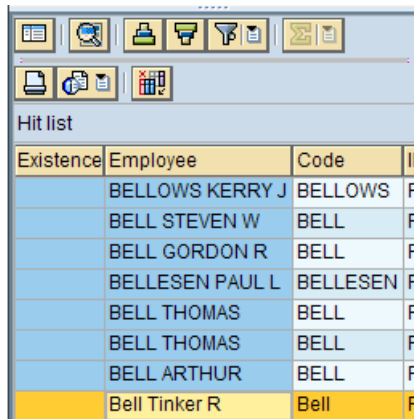
2. Search for position(s). Click on the  button next to 'Person'.



3. In the expanded display, click on the 'Search Term' and fill the resultant "With Name" box with EITHER the person's last name or the person's Pernr. Click the Find Icon.

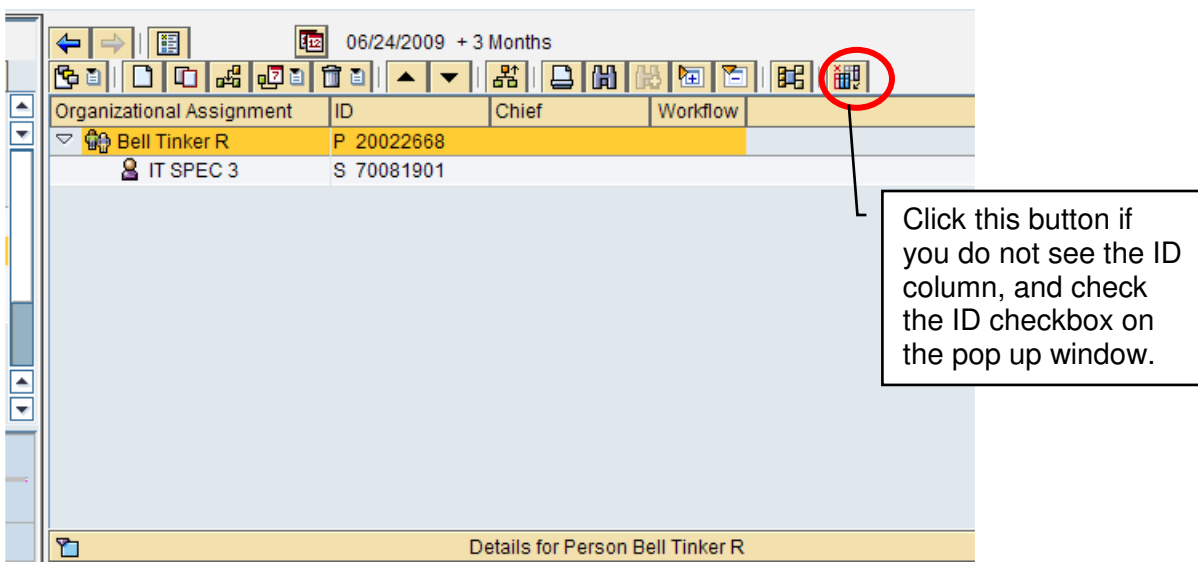


4. Double click on the desired name...



| Existence | Employee | Code | |
|-----------|-----------------|----------|---|
| | BELLOWS KERRY J | BELLOWS | F |
| | BELL STEVEN W | BELL | F |
| | BELL GORDON R | BELL | F |
| | BELLESEN PAUL L | BELLESEN | F |
| | BELL THOMAS | BELL | F |
| | BELL THOMAS | BELL | F |
| | BELL ARTHUR | BELL | F |
| | Bell Tinker R | Bell | F |

5. ...and the Position number shows as the “S” entry under the “ID” column (In the upper right screen quadrant). Verify correct employee.



06/24/2009 + 3 Months

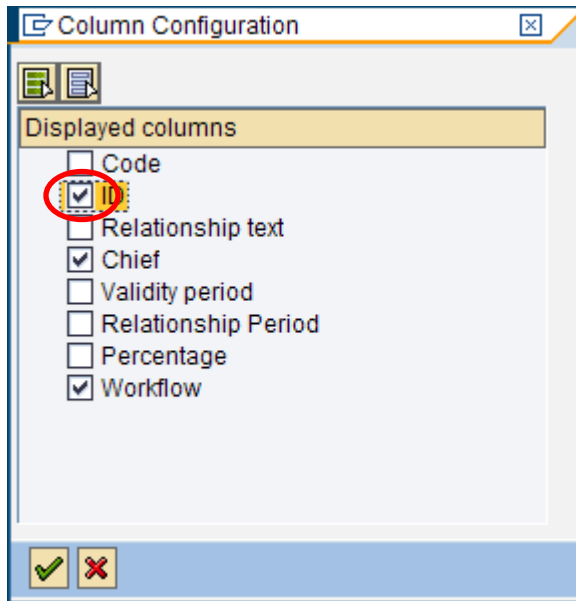
| Organizational Assignment | ID | Chief | Workflow |
|---------------------------|------------|-------|----------|
| Bell Tinker R | P 20022668 | | |
| IT SPEC 3 | S 70081901 | | |

Click this button if you do not see the ID column, and check the ID checkbox on the pop up window.

Details for Person Bell Tinker R

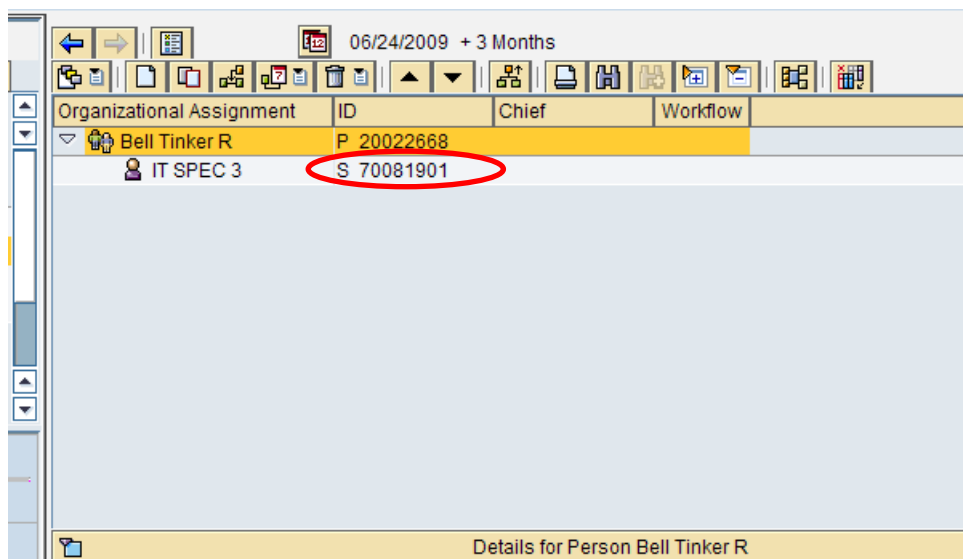
Add the ID column

(If your presentation doesn't show you an ID column, click on the "columns" icon in the box circled in red above. A popup box as shown below will allow you to select columns. Put a checkmark in the "ID" box and click the green checkmark icon in the lower left.)

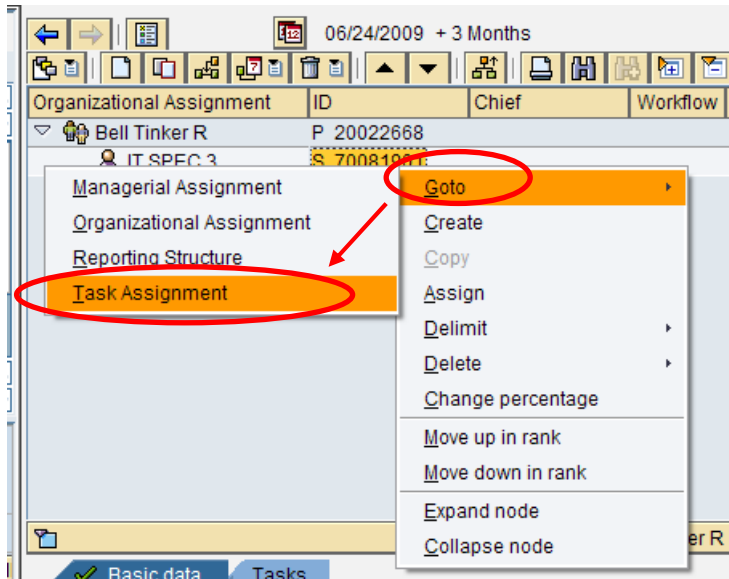


Show currently assigned roles

6. On the information screen shown here, right click on the position number...

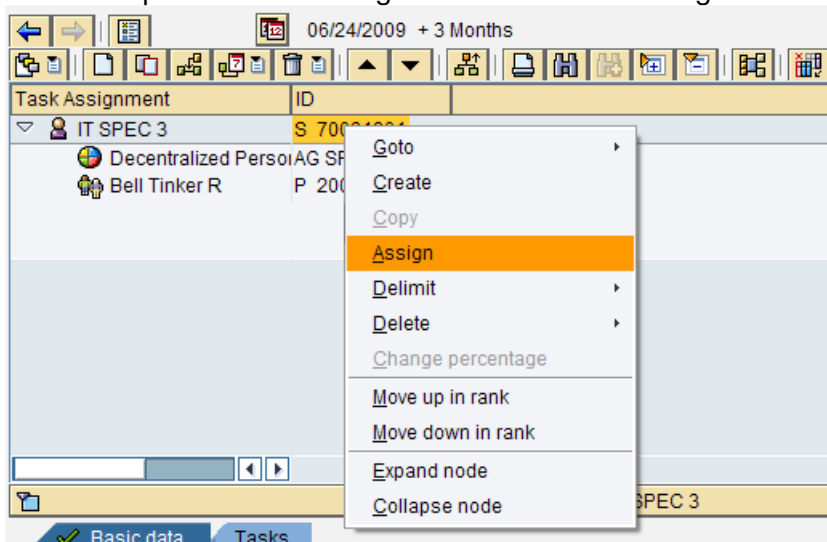


7. Highlighting the resultant “Goto” option will extend a box which allows you to select and click on “Task Assignment” as shown here.

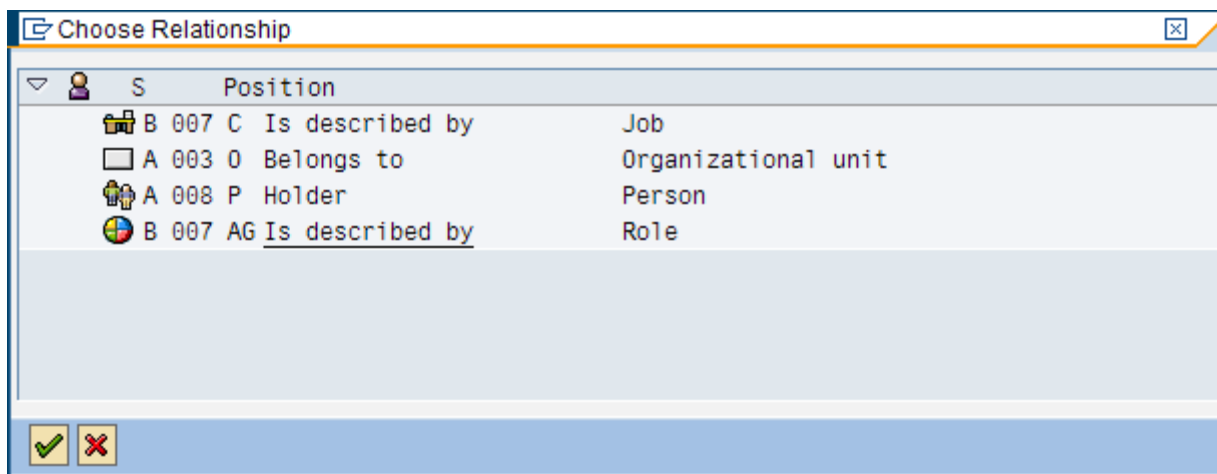


Add roles

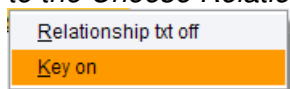
8. This will show you all the professional roles assigned this Position number. To add more, right click on the position number again and select the “Assign”



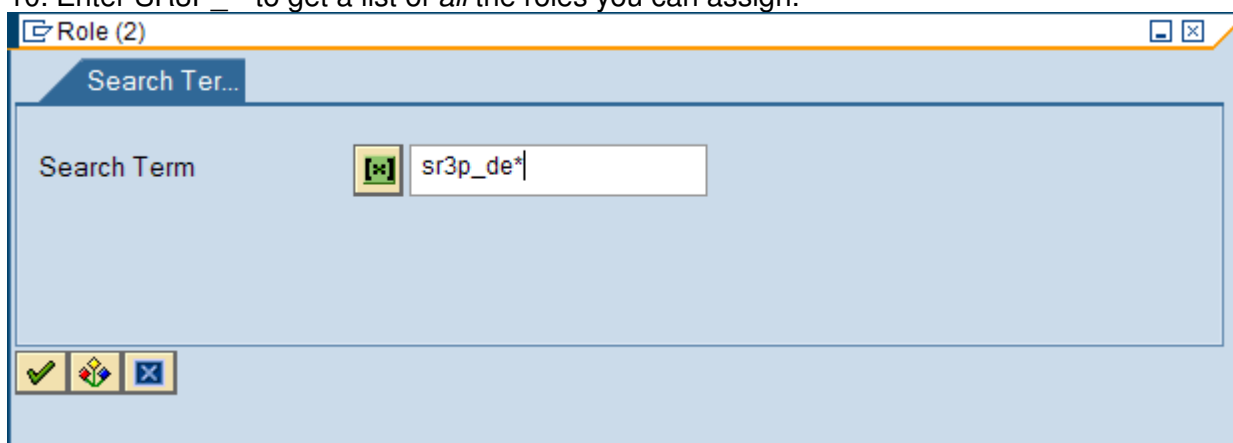
9. “Role” relationships can be assigned by double clicking on the bottom line (Is described by Role) shown here.. (or click the bottom line, then the green arrow...)



NOTE: If you don't see the technical names such as AG next to the *Is described by*, go back to step 8, to the *Choose Relationship* screen. Right click anywhere on the screen and click on *Key on*.

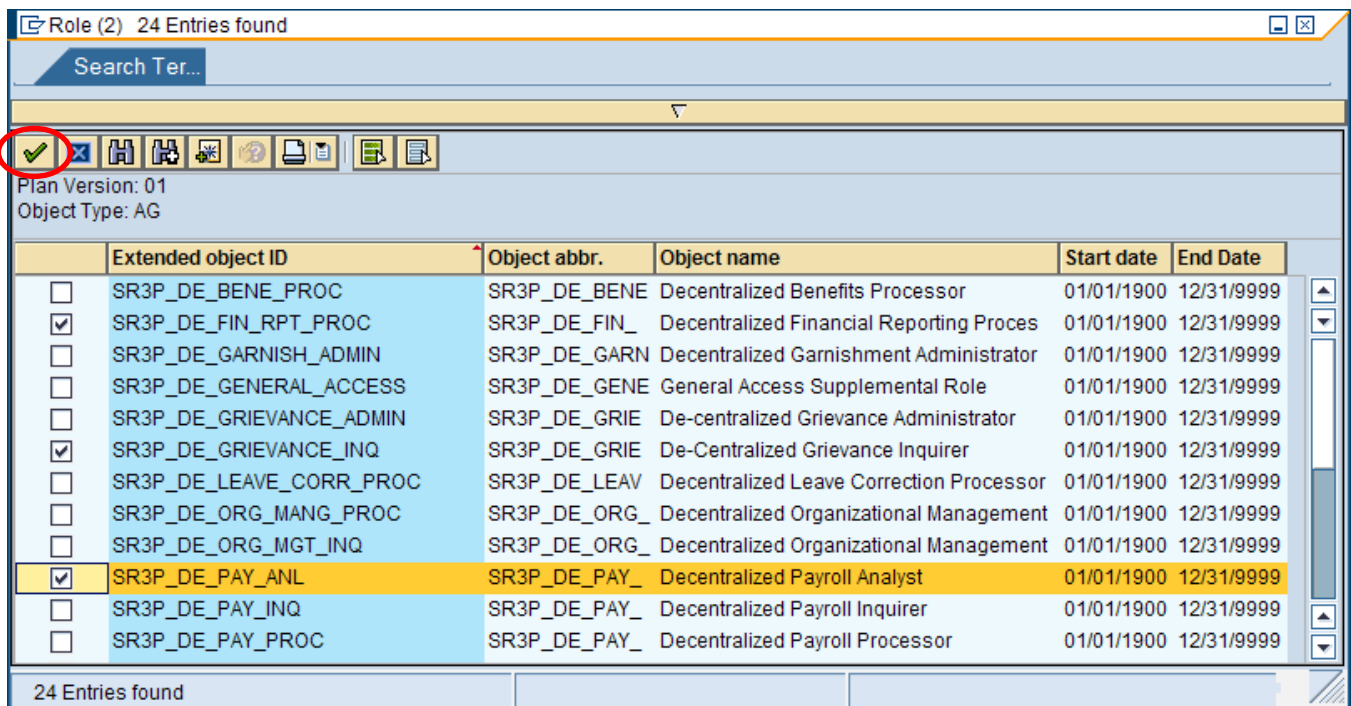


10. Enter SR3P_* to get a list of *all* the roles you can assign.

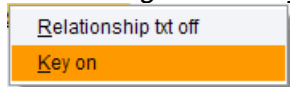


11. In the screen that follows, checkmark the roles that you want to assign to this position.

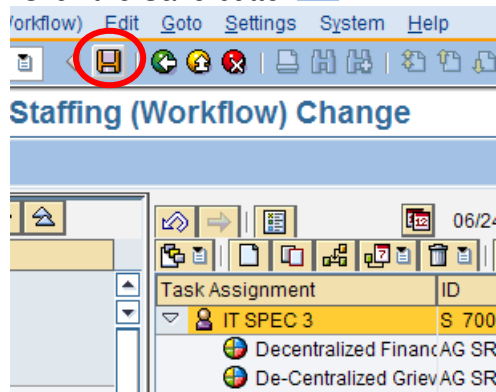
12. Click the Check mark button 



NOTE: If you don't see the Extended object ID column, go back to step 8, to the Choose Relationship screen. Right click anywhere on the screen and click on Key on.





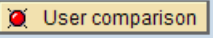
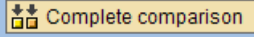
13. Click the Save button

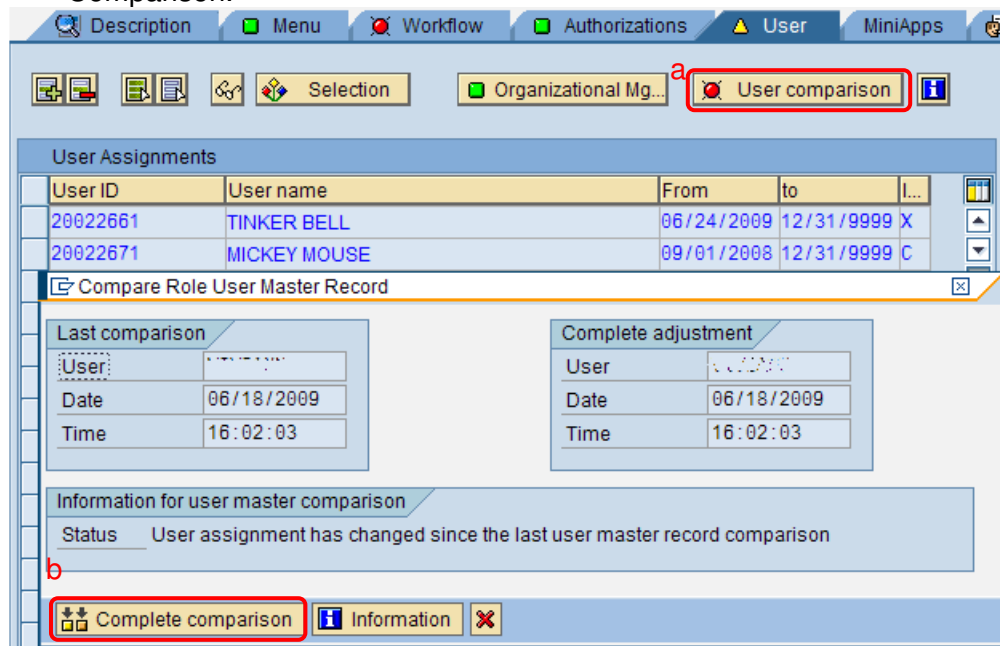


14. To reconcile these newly assigned roles, go to Transaction PFCG, Step 10: Reconciling the Role or complete the next steps.

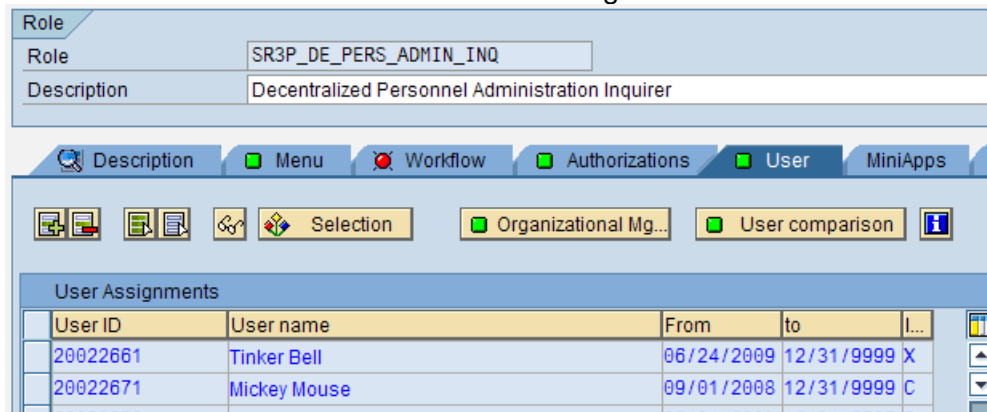
Reconcile the Roles Using SU01D


1. Enter transaction SU01D (/nSU01D)
2. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field, of the employee you just added roles to.
3. Click on  to Display.
4. Click on the Roles tab
5. Double click on the red circle to the left of the newly assigned role.
6. Display roles window opens (this is the PFCG screen)
7. Click on the User tab

8. If the  'User comparison' button is red,
 - a. Click on the  button
 - b. In the Compare Role User Master Record popup, click on  'Complete Comparison.'



9. All buttons within the 'User' tab should now be green.




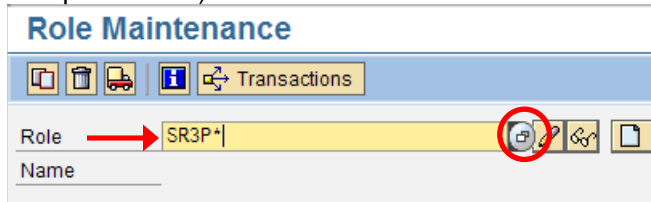
10. Click the 'Save'  button to save changes to the role.
11. Close the Change Roles screen
12. Repeat from step 4 to reconcile any additional roles.
13. Contact your User Administrator after all roles are assigned, they need to go to SU01 and [complete the steps for maintaining a professional user.](#)


Delete Roles from Positions Using PFCG

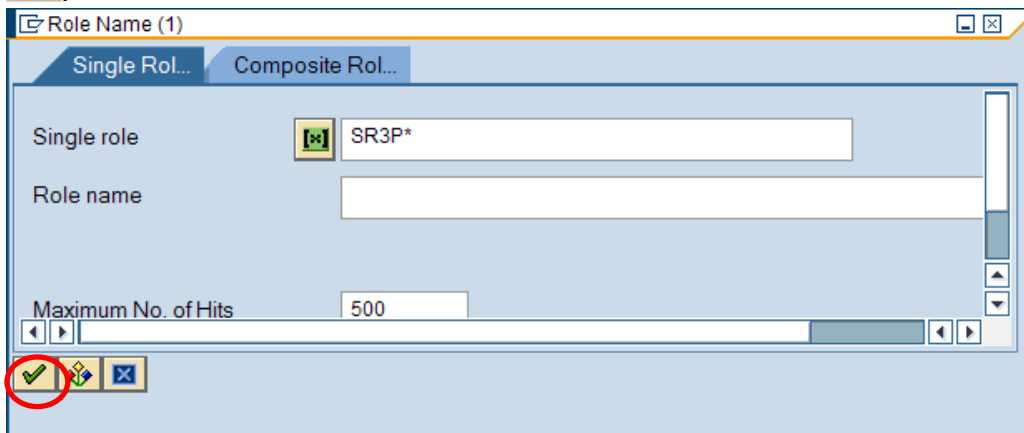
Prerequisites:

- ✓ Role name(s)
- ✓ SAP position number(s).

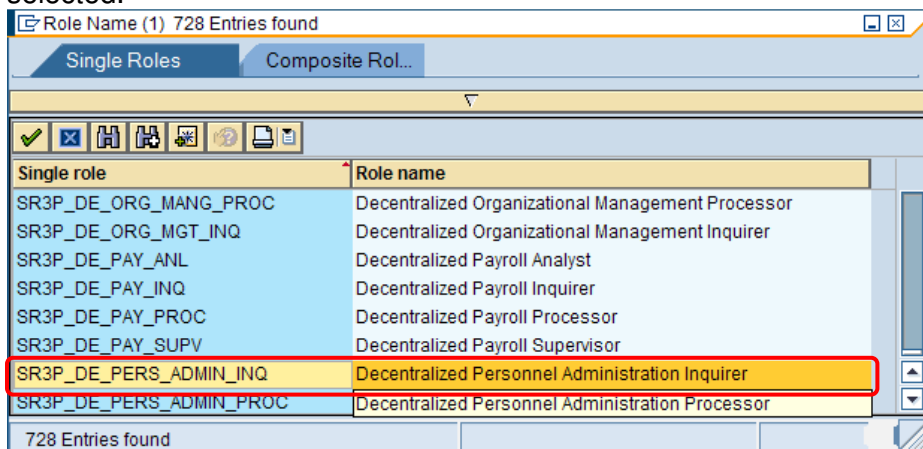
1. Enter transaction '**PFCG**' (/nPFCG) to delete role(s) from position(s).
2. If you know the full role name, enter it in the 'Role' field, and skip to Step 5. Otherwise, search for the role that needs to be deleted from the position. Type SR3P* (for single role) or CR3P* (for composite role) and click on .



3. Verify/confirm the proper tab ('Single Roles' for SR3P*; 'Composite Roles' for CR3P*) and click on .



4. Double click on the appropriate role: for this example, 'Personnel Administration Inquirer' is selected.



| Single role | Role name |
|-------------------------|---|
| SR3P_DE_ORG_MANG_PROC | Decentralized Organizational Management Processor |
| SR3P_DE_ORG_MGT_INQ | Decentralized Organizational Management Inquirer |
| SR3P_DE_PAY_ANL | Decentralized Payroll Analyst |
| SR3P_DE_PAY_INQ | Decentralized Payroll Inquirer |
| SR3P_DE_PAY_PROC | Decentralized Payroll Processor |
| SR3P_DE_PAY_SUPV | Decentralized Payroll Supervisor |
| SR3P_DE_PERS_ADMIN_INQ | Decentralized Personnel Administration Inquirer |
| SR3P_DE_PERS_ADMIN_PROC | Decentralized Personnel Administration Processor |

5. Once the role is selected, click on the edit button.

Role Maintenance

Transactions

Role: SR3P_DE_PERS_ADMIN_INQ [Edit] [Single Role] [Comp. Role]

Name: Decentralized Personnel Administration Inquirer

6. Update the Role

a. Click on the 'User' tab

b. Click on the "Organizational Mg..." button. **IF this button does not appear**, click on the 'back' button, then click 'Goto' pull-down menu (on menu bar), select 'Settings' and select 'Complete View (Org Mgmt & Workflow)'. Then, repeat Step 3 above.

Change Roles

Other role

Role: SR3P_DE_PERS_ADMIN_INQ

Description: Decentralized Personnel Administration Inquirer

Description Menu Workflow Authorizations **User** MiniApps

Selection **Organizational Mg...** User comparison

User Assignments

| User ID | User name | From | to | |
|----------|--------------|------------|------------|---|
| 20022671 | Mickey Mouse | 09/01/2008 | 12/31/9999 | C |
| 20022672 | Minnie Mouse | 09/01/2008 | 12/31/9999 | C |

7. To display SAP position numbers, click on 'View' on the pull-down menu bar, and then click on 'Key On'. Click on the [Key On] to drill down; confirm/verify this change will only impact the correct person and the UserID. If position is "multi-filled", this action will remove access for all employees in this position.

Role: Change Agent Assignment

Indirect user assignments ok

AG SR3P_DE_PERS_ADMIN_INQ Decentralized Personnel Administration I

S 70000664 ADMIN ASSIST 5

S 70000740 HUMAN RESOURCES SPECIALIST

S 70000849 BUS/FIN ADMIN

S 70000850 SR ACCOUNTANT

S 70000913 COMP/FAC COORD

70081901 IT SPEC 3

P 20022668 Bell Tinker R


US 20022661 Tinker Bell

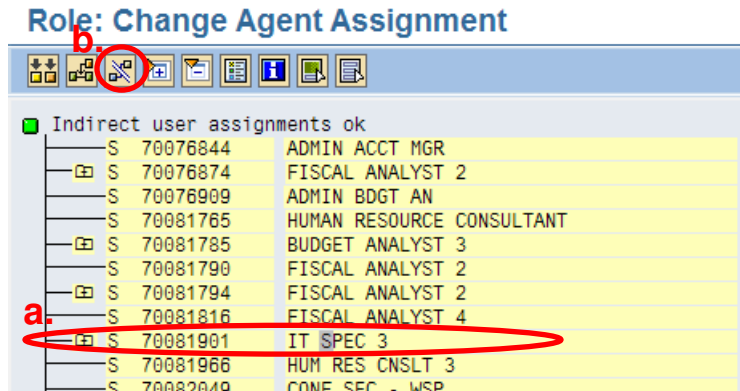
S 70082049 CONF SEC - WSP

S 70082064 BUD&FISC ADMIN

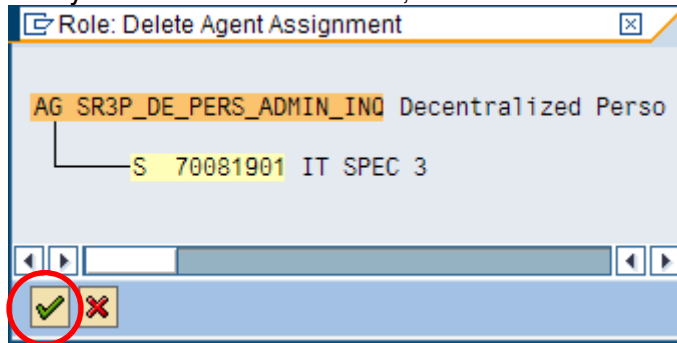
S 70082206 ADMIN ASST 3


S 70082219 FISCAL ANALYST 1

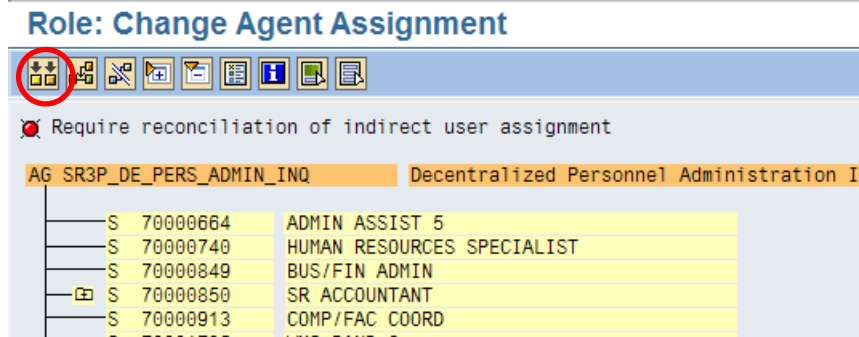
8. Delete the assignment.
 - a. Click on the position name (in yellow) to highlight it.
 - b. Click on the  'Delete Assignment' button.



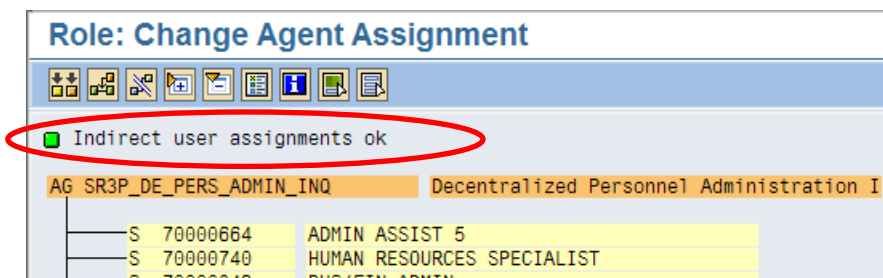
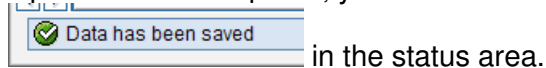
9. Verify all information is correct, and click the 'enter' button.



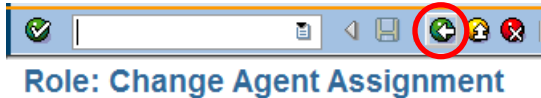
10. Notice the red light and message at the top of the screen; click on the  'indirect user assignment reconciliation' button to turn the light green.



Upon successful update, you will see that the light has turned green, and the message

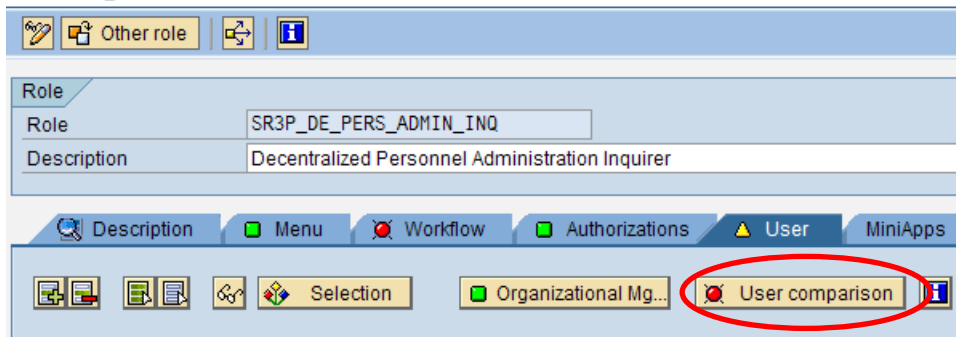


11. Back out of this screen

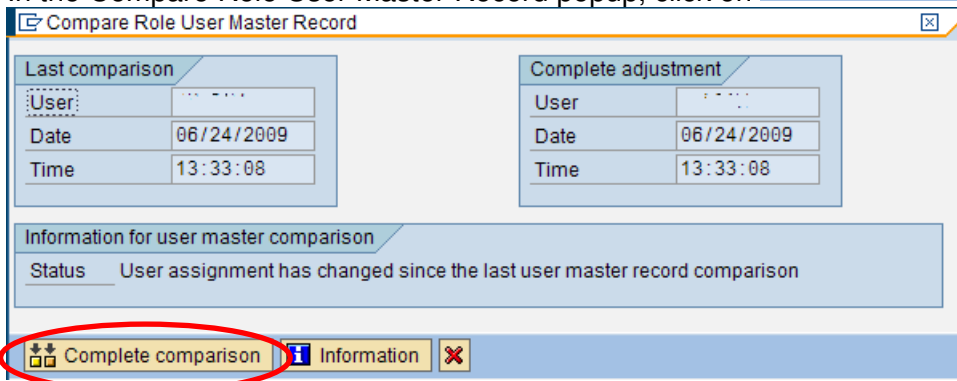


12. If the  User comparison button is red, click on the  User comparison button.

Change Roles

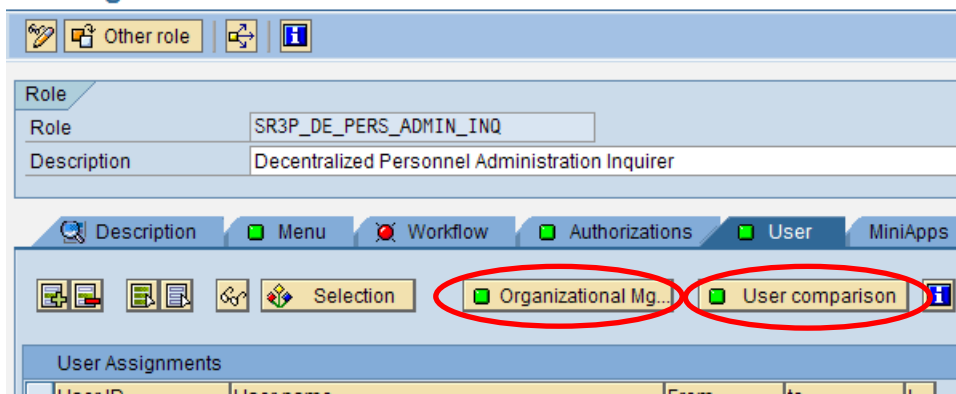




13. In the Compare Role User Master Record popup, click on .



14. All buttons on the 'User' tab should now be green.

Change Roles



15. Click  to save your changes. You will see the message  in the status area.

16. Follow the same steps for [Delete Roles from Positions \(PFCG\)](#) to delete any other roles.

17. If the person is no longer going to be a professional user, contact your User Administrator, they need to go to SU01 and complete the steps for [transferring a professional user back to ESS user](#).

HCM User Administrator

SR3P_XXXX_USER_ADMIN

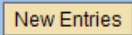
Maintaining a Professional HCM UserID Account

Agency User Administrators will use this process when changing a non-professional (ESSUSER) UserID account to a professional (WA_XXXX) UserID account in order to access HCM.

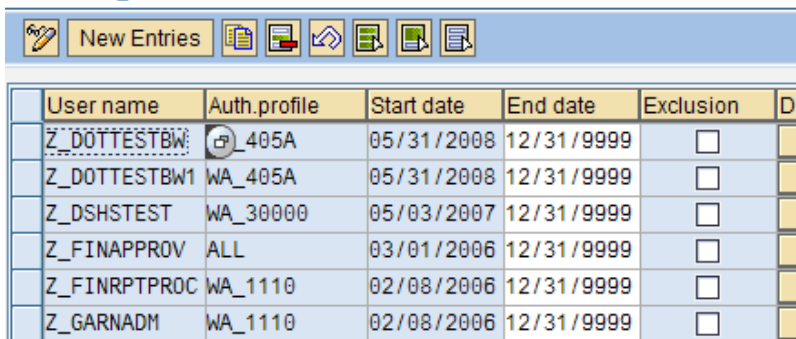
Prerequisites:

- ✓ Professional roles must be assigned to the employee's position by the agency [Auth Administrator](#).


Enter OOSB Auth Profile

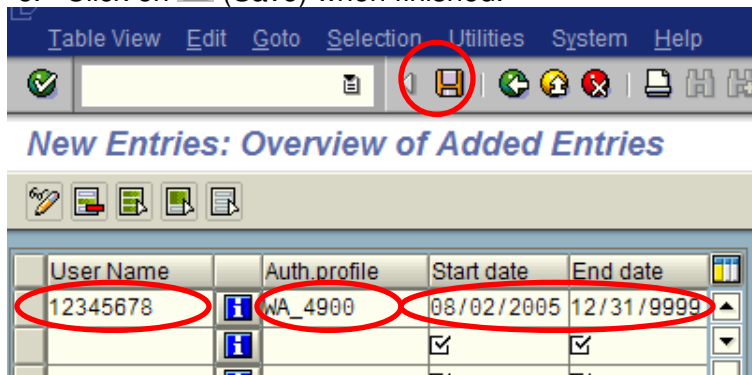
1. Enter transaction 'OOSB' (/nOOSB) to update table T77UA.
2. Click on  (New Entries) to enter the UserID.

Change View "User Authorizations": Overview




| User name | Auth.profile | Start date | End date | Exclusion | Dis |
|--------------|--------------|------------|------------|--------------------------|-----|
| Z_DOTTESTBW | 405A | 05/31/2008 | 12/31/9999 | <input type="checkbox"/> | |
| Z_DOTTESTBW1 | WA_405A | 05/31/2008 | 12/31/9999 | <input type="checkbox"/> | |
| Z_DSHSTEST | WA_30000 | 05/03/2007 | 12/31/9999 | <input type="checkbox"/> | |
| Z_FINAPPROV | ALL | 03/01/2006 | 12/31/9999 | <input type="checkbox"/> | |
| Z_FINRPTPROC | WA_1110 | 02/08/2006 | 12/31/9999 | <input type="checkbox"/> | |
| Z_GARNADM | WA_1110 | 02/08/2006 | 12/31/9999 | <input type="checkbox"/> | |

3. Enter the following:
 - a. User Name – the UserID (Personnel number, **including** leading zeros)
 - b. Auth. Profile – The User Group authorization profile (like: WA_4900);
* Note **Pers Admin Processors require a 2nd entry w/Auth profile 'WA_SOW'.**
 - c. Start Date
 - d. End Date – if an exact date is known it should be entered, otherwise use 12/31/9999
 - e. Click on  (Save) when finished.





| User Name | Auth.profile | Start date | End date |
|-----------|--------------|------------|------------|
| 12345678 | WA_4900 | 08/02/2005 | 12/31/9999 |

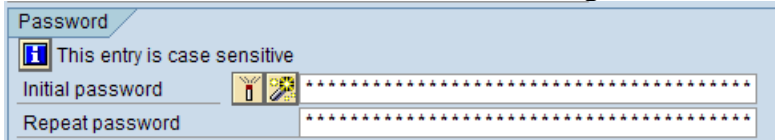
4. Upon successful save the following message will appear


 Data was saved

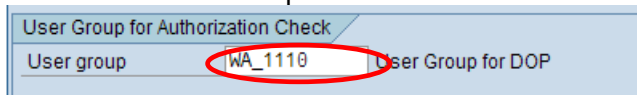
Update the UserID (SU01)

5. Enter transaction SU01
6. Enter the UserID (8 digit personnel number with leading zeros)
7. Click the Display button  to verify the user
8. Click on  to enter Edit mode
9. From the 'Logon data' tab, update the following:
 - a. Enter an initial password manually. The password must follow the hardened guidelines (8 characters which contain at least 1 digit, and 1 special character.)

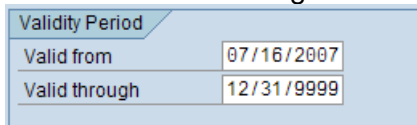
NOTE: DO NOT use the wizard. It will generate a 40 digit password.



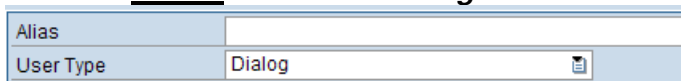
- b. Enter the User Group for your Agency. To search, click on the  button to search for your User Group.



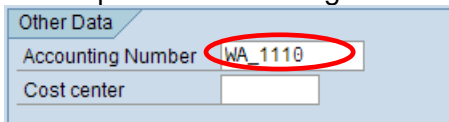
- c. Verify there are Validity Period dates, if there are no dates enter them as follows –
 1. Valid from – date of creation
 2. Valid through – 12/31/9999



- d. Verify that the User Type is set to 'Dialog' - **this is very important, as the UserID will not work unless it is set to 'Dialog'.**



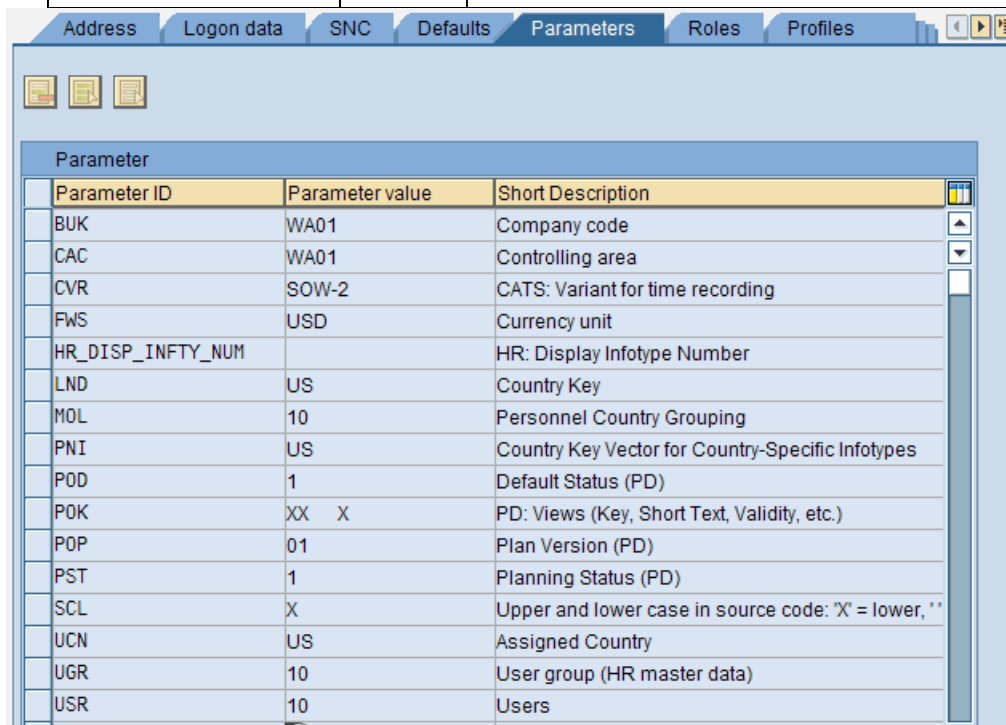
- e. Populate "Accounting Number" field in "Other Data" with User Group data from 9b above



10. Click on the Parameters tab and check the parameters. There should be 16 parameters entered, if the parameters are not entered enter the following parameters:

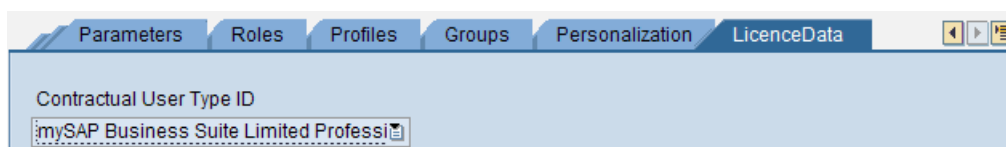
NOTE: Enter only the Parameter ID and Value and then press enter.

| Parameter ID | Value | Short Description |
|--------------------|-------|--|
| BUK | WA01 | Company code |
| CAC | WA01 | Controlling area |
| CVR | SOW-2 | Variant for time recording |
| FWS | USD | Currency unit |
| HR_DISP_INFITY_NUM | | HR: Display Infotype Number |
| LND | US | Country key |
| MOL | 10 | Personnel Country Grouping |
| PNI | US | Country Key Vector for Country-Specific Infotypes |
| POD | 1 | Default Status (PD) |
| POK | XX | PD: Views (Key, Short Text, Validity, etc.) |
| POP | 01 | Plan Version (PD) |
| PST | 1 | Planning Status (PD) |
| SCL | X | Upper and lower case in source code: 'X' = lower, '' = upper |
| UCN | US | Assigned Country |
| UGR | 10 | User group (HR master data) |
| USR | 10 | Users |



The screenshot shows the SAP Parameters tab with a list of 16 parameters. The table has three columns: Parameter ID, Parameter value, and Short Description. The parameters are: BUK (WA01, Company code), CAC (WA01, Controlling area), CVR (SOW-2, CATS: Variant for time recording), FWS (USD, Currency unit), HR_DISP_INFITY_NUM (, HR: Display Infotype Number), LND (US, Country Key), MOL (10, Personnel Country Grouping), PNI (US, Country Key Vector for Country-Specific Infotypes), POD (1, Default Status (PD)), POK (XX X, PD: Views (Key, Short Text, Validity, etc.)), POP (01, Plan Version (PD)), PST (1, Planning Status (PD)), SCL (X, Upper and lower case in source code: 'X' = lower, '' = upper), UCN (US, Assigned Country), UGR (10, User group (HR master data)), and USR (10, Users).

| Parameter ID | Parameter value | Short Description |
|--------------------|-----------------|--|
| BUK | WA01 | Company code |
| CAC | WA01 | Controlling area |
| CVR | SOW-2 | CATS: Variant for time recording |
| FWS | USD | Currency unit |
| HR_DISP_INFITY_NUM | | HR: Display Infotype Number |
| LND | US | Country Key |
| MOL | 10 | Personnel Country Grouping |
| PNI | US | Country Key Vector for Country-Specific Infotypes |
| POD | 1 | Default Status (PD) |
| POK | XX X | PD: Views (Key, Short Text, Validity, etc.) |
| POP | 01 | Plan Version (PD) |
| PST | 1 | Planning Status (PD) |
| SCL | X | Upper and lower case in source code: 'X' = lower, '' = upper |
| UCN | US | Assigned Country |
| UGR | 10 | User group (HR master data) |
| USR | 10 | Users |



The screenshot shows the SAP Parameters tab with the 'Contractual User Type ID' field. The field contains the text 'mySAP Business Suite Limited Professi'.

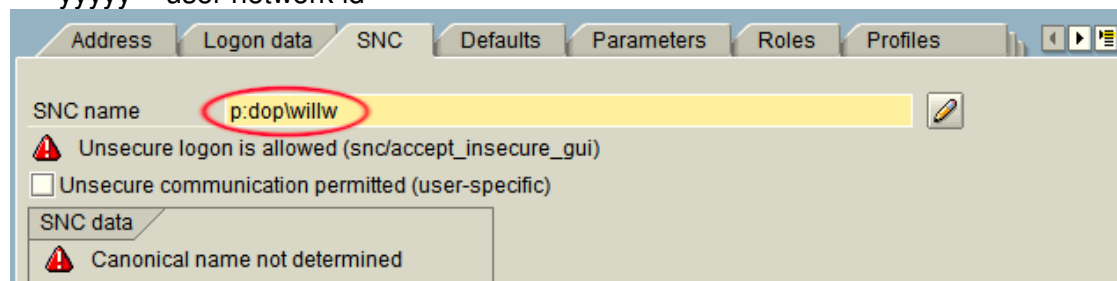
11. Save  the account


If **NOT** using Single Sign On (SSO) you are done. If you **ARE** using SSO continue to step 14.

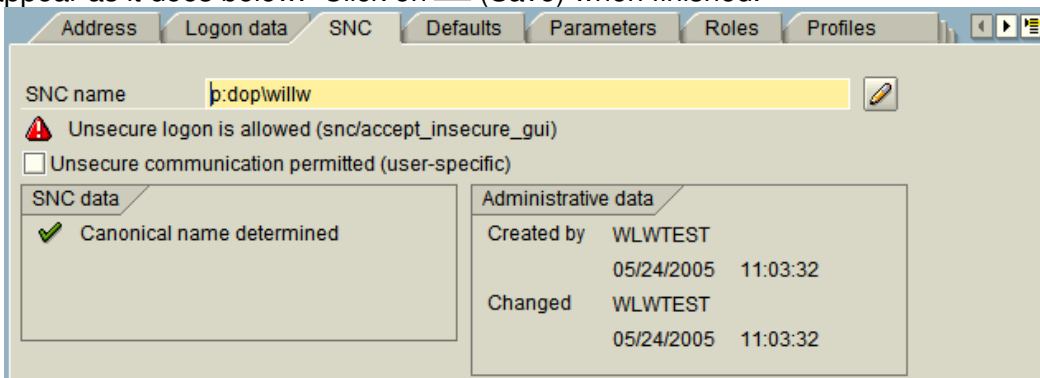
Single Sign On (SSO)

12. Click the “SNC” tab. Enter the SNC name in the following format ‘p:xxx\yyyy’ (see example below).

- xxx = 3 letter agency code
- yyyy = user network id





13. If the update is successful, a green check mark and the message “Canonical name determined” will appear as it does below. Click on  (Save) when finished.



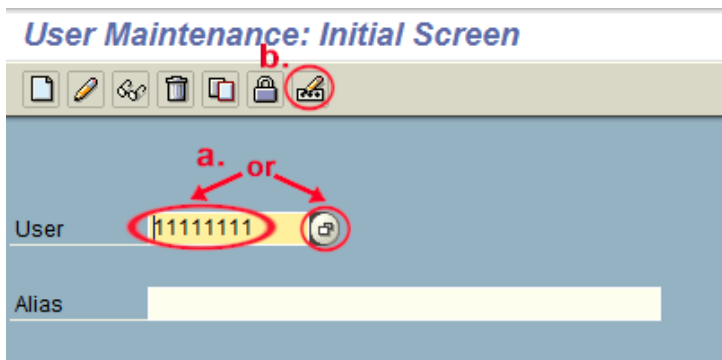
HCM UserID Maintenance


Reset HCM Password (SU01)

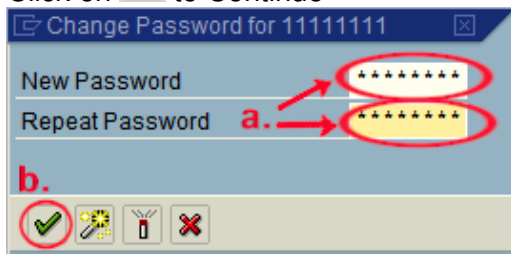
1. Enter transaction ‘**SU01**’ (/nSU01) to reset the password
2. Enter the UserID for which you are re-setting the password.
 - a. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the ‘User’ field. In this example it is ‘11111111’. To search for the User, click on  to search and select the User.

NOTE: Users will not be unlocked by resetting the password so always check if the user is locked by clicking on the  Lock button. Unlock the user if needed.

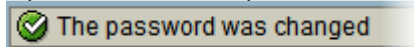
- b. Click on  to Change Password or Shift + F8




3. Enter the new password **Manually**
 - a. Enter the new password and repeat for verification (Hardened password standards apply; passwords must contain at least one letter, one number, one special character and be at least eight characters long)
 - b. Click on  to Continue



4. Upon successful update the following message will be displayed. Notify User of new password.



Lock/Unlock HCM UserID (SU01)

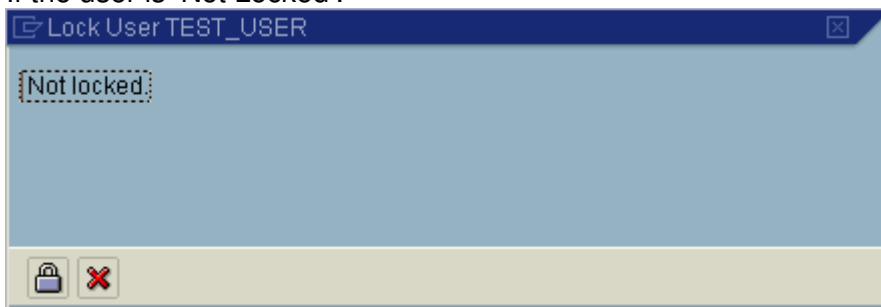
1. Enter transaction 'SU01' (/nSU01) to lock or unlock a UserID
2. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) that needs to be locked or unlocked into the 'User' field. In this example it is '11111111'. Click the  'Lock/Unlock' button.

User Maintenance: Initial Screen



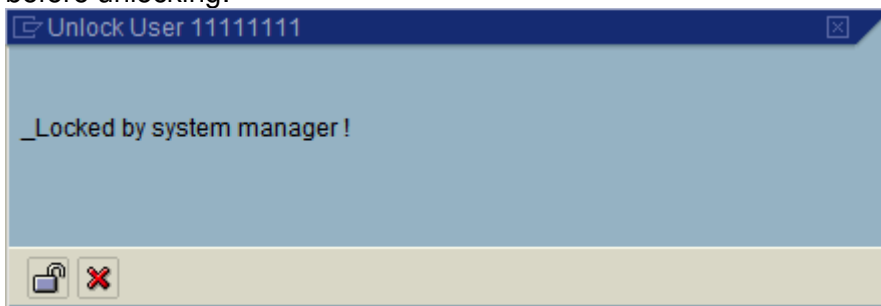
The screenshot shows the 'User Maintenance: Initial Screen' in SAP. At the top, there is a toolbar with icons for document, edit, delete, and lock/unlock. The lock/unlock icon is circled in red. Below the toolbar, there are two input fields: 'User' and 'Alias'. The 'User' field contains the value '11111111' and has a small lock/unlock icon to its right. The 'Alias' field is empty.

3. A screen indicating the Lock Status of the User will appear.
 - a. If the user is 'Not Locked':



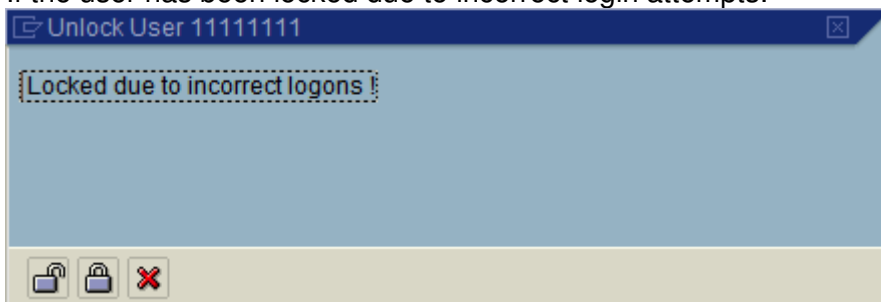
The screenshot shows a dialog box titled 'Lock User TEST_USER'. The main area of the dialog contains the text 'Not locked.' in a dashed box. At the bottom, there are two buttons: a lock icon and a red 'X' icon.

- b. If the user has been locked by the System Manager, there may be a specific reason, research before unlocking:



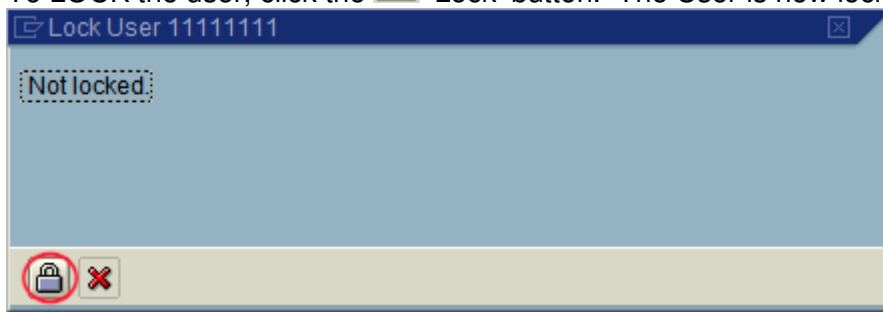
The screenshot shows a dialog box titled 'Unlock User 11111111'. The main area of the dialog contains the text '_ Locked by system manager !' in a dashed box. At the bottom, there are two buttons: a lock icon and a red 'X' icon.


- c. If the user has been locked due to incorrect login attempts:

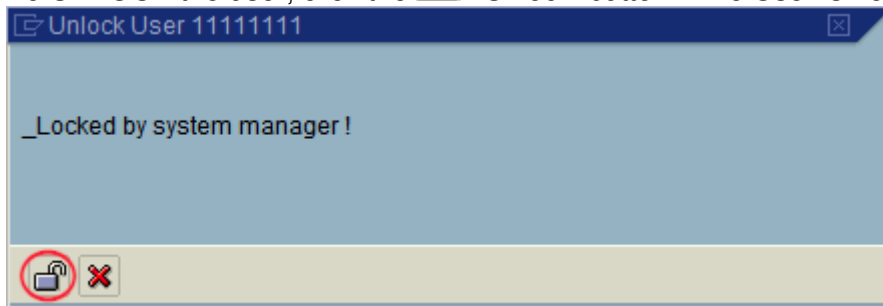


The screenshot shows a dialog box titled 'Unlock User 11111111'. The main area of the dialog contains the text 'Locked due to incorrect logons !' in a dashed box. At the bottom, there are three buttons: a lock icon, an open lock icon, and a red 'X' icon.

4. To LOCK the user, click the  'Lock' button. The User is now locked.



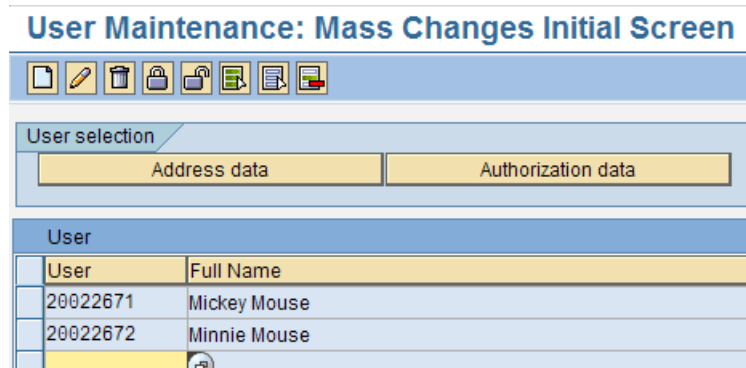
5. To UNLOCK the user, click the  'Unlock' button. The User is now unlocked.



Mass HCM UserID Lock/Unlock (SU10)

There are many options for Mass User Maintenance, including locking of UserIDs, changing Parameters and/or Defaults, etc.

1. Enter transaction '**SU10**' (/nSU10) to lock or unlock multiple UserIDs
2. Select the Users to be Unlocked.
Option 1 – Enter the users manually
 - a. Enter the UserIDs (8 digit personnel number **including** leading zeroes) manually into the User Field




- b. Click the Lock  or Unlock  button, depending on whether you need to lock or unlock the users.

Option 2 – Select Users from a list

- Click on the Authorization data button


User Maintenance: Mass Changes Initial Screen

The screenshot shows a toolbar with icons for file operations and a 'User selection' section. Below this, there are two buttons: 'Address data' and 'Authorization data'. The 'Authorization data' button is highlighted with a red rectangle.

- Search on the User Group (like WA_1110). You can also search using any of the other options to refine the results.
- Enter the 'Group for Authorization', in this example it is XYZ_123. This would be your specific Agency's User Group.
- Click on  to execute the search.

Users by Complex Selection Criteria

The screenshot shows a form titled 'Selection criteria for user'. It has three fields: 'User', 'Group for authorization', and 'User group (general)'. The 'Group for authorization' field is highlighted with a red rectangle and contains the text 'XYZ_123'. To the right of the fields are three arrows pointing right.

- Select and Transfer the Users to update
- Click on the  (Select All button) or select individual users
- Click on the Transfer button

The screenshots show two instances of the 'Users by Complex Selection Criteria' table. Both tables have a toolbar at the top with a 'Transfer' button highlighted by a red rectangle. The tables show a list of users with columns: User, Full Name, Group, Account no, Locked, Valid from, Valid to, User Type, and Ref. User. The first table shows 4 users selected, and the second table shows 4 users selected. A red arrow points from the 'User Type' column in the first table to the 'User Type' column in the second table.

| User | Full Name | Group | Account no | Locked | Valid from | Valid to | User Type | Ref. User |
|----------|------------|---------|------------|--------|------------|----------|-----------|-----------|
| 11111111 | First Last | XYZ_123 | | | | | A Dialog | |
| 11111112 | First Last | XYZ_123 | | | | | A Dialog | |
| 11111113 | First Last | XYZ_123 | | | | | A Dialog | |
| 11111114 | First Last | XYZ_123 | | | | | A Dialog | |


h. To LOCK Selected Users

- Click on  to Lock all the Users selected


User Maintenance: Mass Changes Initial Screen

The screenshot shows the 'User Maintenance: Mass Changes Initial Screen' with the 'Authorization data' button selected. Below the buttons, there is a table with columns: User, Full Name, and a lock icon. The first row of the table is highlighted with a red circle, and the lock icon in the first row is also highlighted with a red circle.

| User | Full Name |
|----------|------------|
| 11111111 | First Last |
| 11111112 | First Last |
| 11111113 | First Last |
| 11111114 | First Last |
| 11111115 | First Last |


2. A log screen similar to the one below will appear. Click on the Expand button  ; the expanded view will give a detailed log of each user that was locked

Log Display

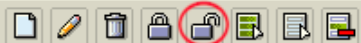


| Overview | Number |
|------------------------------------|--------|
| Mass user changes | 1 |
| System: HRD Client: 700 | 1 |
| Executed by: First Last (USERID) | 1 |
| ▶ Date: 07/07/2009, time 16:33:50. | 8 |

i. To UNLOCK Selected Users

1. Click on  to Unlock all the Users selected


User Maintenance: Mass Changes Initial Screen




User selection

Address data Authorization data

| User | Full Name |
|----------|------------|
| 11111111 | First Last |
| 11111112 | First Last |
| 11111113 | First Last |
| 11111114 | First Last |
| 11111115 | First Last |

2. A log screen similar to the one below will appear. Click on the Expand button  ; the expanded view will give a detailed log of each user that was unlocked

Log Display




| Overview | Number |
|------------------------------------|--------|
| Mass user changes | 1 |
| System: HRD Client: 700 | 1 |
| Executed by: First Last (USERID) | 1 |
| ▶ Date: 07/07/2009, time 16:33:50. | 8 |

Non-Professional Users (ESS Users) Leave State Employment – Employee Status is Withdrawn:




NOTE: DOP recommends to keep the SU01 UserID account for withdrawn employees for at least 30 days after the termination of state employment. This account gives the user the authorizations to see their earnings statement in the Portal.

HCM:

1. Login to HCM – HRMS Production (RP0) – through the SAP Logon Pad
2. Verify the employee is withdrawn

1. Enter transaction PA20
2. Enter employee's personnel number
3. Click the Overview button 
4. Check the Status: Withdrawn

| | | | |
|----------|----------------------------|------------|-----------------------|
| Name | [Employee Name] | | |
| PersArea | 4650 Parks/Recreation Comm | EEGroup | H Non-Perm. Limited |
| PSubarea | 0001 Non Represented | EESubgroup | 05 H-OT Elig>40hrs/wk |
| Status | Withdrawn | | |

3. Enter transaction 'SU01' (/nSU01)
4. Enter the UserID (Personnel Number, **including** leading zeroes) into the 'User' field.
5. Click the Display button  to verify the user
6. Click on the Back button  to go back to the User Maintenance screen
7. Click the Delete button  and delete the account.


NOTE: Portal User Administrator needs to delete personnel number UserID from the Portal.

Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):

HCM:

1. Login to HCM – HRMS Production (RP0) – through the SAP Logon Pad

*If the employee's employment status is **active or inactive (PA20)**, and no longer in your agency*

2. Verify the employee status is active/inactive
 1. Enter transaction PA20
 2. Enter employee's personnel number
 3. Click the Overview button 
 4. Check the Status: Active or Inactive

| | | | |
|----------|-----------------------|------------|------------------------|
| Name | [Employee Name] | | |
| PersArea | 1000 Attorney General | EEGroup | B Civil Service Exempt |
| PSubarea | 0001 Non Represented | EESubgroup | 01 Monthly(M) OT Exem |
| Status | Active | | |

| | | | |
|----------|--------------------------|------------|-----------------------|
| Name | [Employee Name] | | |
| PersArea | 2450 Military Department | EEGroup | 0 Permanent |
| PSubarea | 0001 Non Represented | EESubgroup | 01 Monthly(M) OT Exem |
| Status | Inactive | | |


3. Enter transaction 'OOSB' to remove the authorization (/nOOSB).
 - a. Click the "Position" button at the bottom of the screen and enter the eight digit UserID in the User name field and click the green check mark. That will position the list to the selected UserID

Change View "User Authorizations": Overview

| User name | Auth.profile | Start date | End date | Exclusion | Display |
|-------------|---------------|------------|------------|--------------------------|---------|
| Z_WSPTEST | WA_2250 | 03/30/2006 | 12/31/9999 | <input type="checkbox"/> | |
| Z_WSPTESTBW | WA_2250 | 03/30/2006 | 12/31/9999 | <input type="checkbox"/> | |
| Z_WSPTEST | Another entry | | | | |
| Z_WSPTEST | User name | | | | |
| Z_WSPTEST | Auth.profile | | | | |
| Z_WSPTEST | Start date | | | | |
| Z_WSPTEST | | | | | |
| Z_WSPTEST | | | | | |







Position... Entry 3,180 of 3,189

b. Click the box to the left of the UserID

c. Click  to delete the entry. Repeat for all entries for this UserID that are associated with the user's access in **your** agency/personnel area.

Change View "User Authorizations": Overview



c.

 New Entries     

| | User name | Auth.profile | Start date | End date | Exclusion | Di |
|-----------|--------------|--------------|------------|------------|--------------------------|----|
| | Z_DOTTESTBW | WA_405A | 05/31/2008 | 12/31/9999 | <input type="checkbox"/> | |
| | Z_DOTTESTBW1 | WA_405A | 05/31/2008 | 12/31/9999 | <input type="checkbox"/> | |
| b. | Z_SHSTEST | 30000 | 05/03/2007 | 12/31/9999 | <input type="checkbox"/> | |
| | Z_FINAPPROV | ALL | 03/01/2006 | 12/31/9999 | <input type="checkbox"/> | |
| | Z_FINRPTPROC | WA_1110 | 02/08/2006 | 12/31/9999 | <input type="checkbox"/> | |

You will see  Number of deleted entries: 1 in the status area.

d. Click the Save button  to save the table.

- Enter transaction 'SU01' (/nSU01) to update the UserID.
- Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field.
- Click on the Display button , and verify the user.
- In the Logon Data tab; Click on Display/Change button  to enter the edit mode.
- Change the UserGroup back to ESSUSER.

User Group for Authorization Check

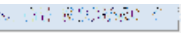
User group **ESSUSER** User group for ESS user

- Click on Save button  to save the account.

If the employee's employment status is withdrawn (PA20)




- Verify the employee is Withdrawn
 - Enter transaction PA20
 - Enter employee's personnel number

- c. Click the Overview button 
- d. Check the Status: Withdrawn

| | | | | | |
|----------|---|-----------------------|------------|----|--------------------|
| Name |  | | | | |
| PersArea | 4650 | Parks/Recreation Comm | EEGroup | H | Non-Perm. Limited |
| PSubarea | 0001 | Non Represented | EESubgroup | 05 | H-OT Elig>40hrs/wk |
| Status | Withdrawn | | | | |

2. Remove OOSB entries (See above for instructions)



NOTE: DOP recommends to keep the SU01 UserID account for withdrawn employees for at least 30 days after the termination of state employment. This account gives the user the authorizations to see their earnings statement in the Portal.


3. Enter transaction 'SU01' (/nSU01)
4. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field.
5. Click the Display button  to verify the user.
6. Click on the Back button  to go back to the User Maintenance screen.
7. Click the Delete button  and delete the account.

NOTE: BI, E-Recruiting and Portal User Administrators need to do clean up on these professional user accounts if the users had access to those systems.


Employee has a Name Change

NOTE: When an employee has a name change and the HCM personnel master record is updated, this change does not update the UserID account (SU01) for that employee in HCM. The Agency User Administrator must manually go into SU01 and change employee's name.

1. Enter transaction SU01
2. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field.
3. Click the Display button  to verify the user.
4. Click on the Display/Change button  to enter the edit mode.

| | | | | | | | | | | | | | |
|----------------|---|------------|--|-----|--|----------|--|------------|--|-------|--|----------|--|
| Address | | Ligon data | | SNC | | Defaults | | Parameters | | Roles | | Profiles | |
| Person | | | | | | | | | | | | | |
| Title |  | | | | | | | | | | | | |
| Last name | Doe | | | | | | | | | | | | |
| First name | Jane | | | | | | | | | | | | |
| Academic Title | | | | | | | | | | | | | |
| Format | Jane Doe | | | | | | | | | | | | |


5. Change Last and/or First name

| | | | | | | | | | | | | | |
|------------|---|------------|--|-----|--|----------|--|------------|--|-------|--|----------|--|
| Address | | Ligon data | | SNC | | Defaults | | Parameters | | Roles | | Profiles | |
| Person | | | | | | | | | | | | | |
| Title |  | | | | | | | | | | | | |
| Last name | Jackson | | | | | | | | | | | | |
| First name | Jane | | | | | | | | | | | | |

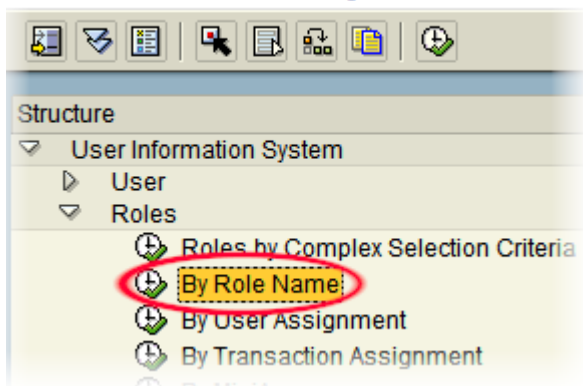
6. Click on Save  to save the account.



HCM Security Auditor
SR3P_XXXX_SECURITY_AUDIT

Display Users by Role (SUIM)

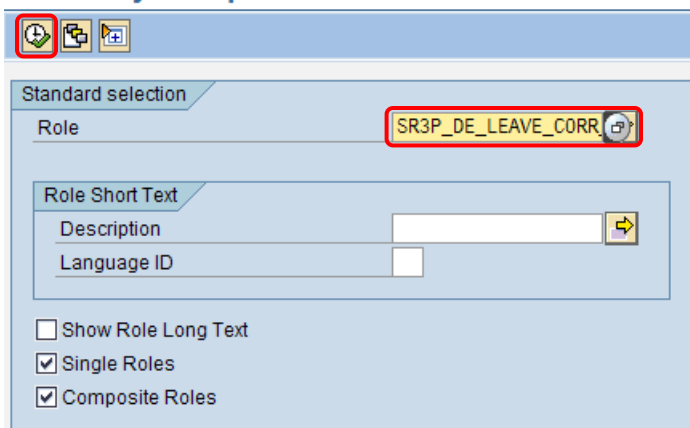
1. Enter transaction 'SUIM' (/nSUIM) to Display Users by Role
2. Display Users for a Specific Role
3. From the User Information System screen, drill down to Roles > By Role Name and click on  to Execute.


User Information System



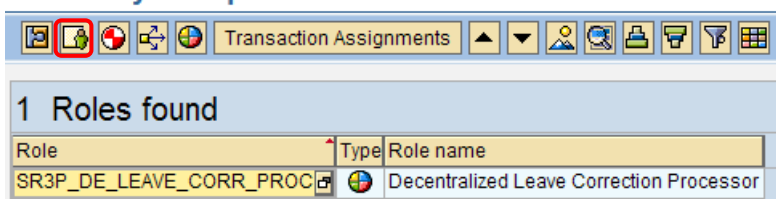
4. Enter the role name (or search if you don't know it) and click on  to Execute. To search for the Role, enter SR3P* in the Role field and click on  to search.


Roles by Complex Selection Criteria



5. From the Roles by Complex Selection Criteria screen, select  User Assignment to display all users assigned to the selected role.

Roles by Complex Selection Criteria



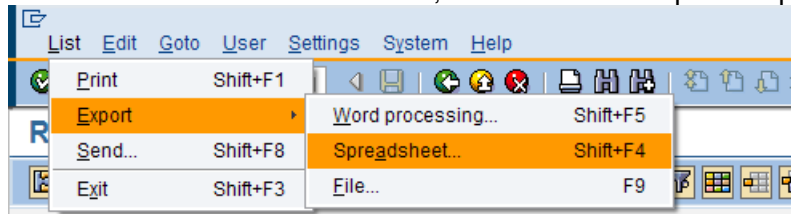
| Role | Type | Role name |
|-------------------------|---|--|
| SR3P_DE_LEAVE_CORR_PROC |  | Decentralized Leave Correction Processor |


6. A list of Users will be generated.

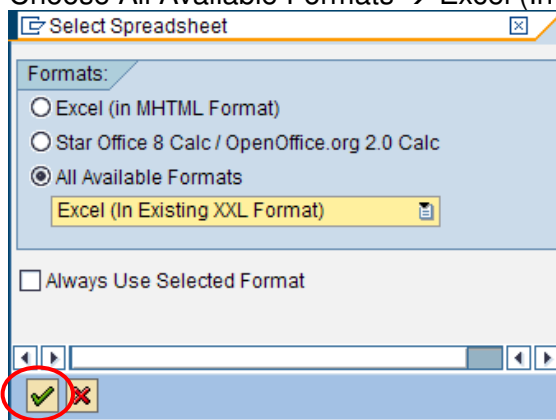
Roles by Complex Selection Criteria

| Number of Users Selected:345 | | | | | | | | |
|------------------------------|---------------|------------|-------------|--------|------------|---------------|-----------|-----------|
| User | Complete name | User group | Account no. | Locked | Valid from | Valid through | User Type | Ref. User |
| WA_4950 | WA_4950 | WA_4950 | WA_4950 | | | | A Dialog | |
| WA_4950 | WA_4950 | WA_4950 | WA_4950 | | | | A Dialog | |

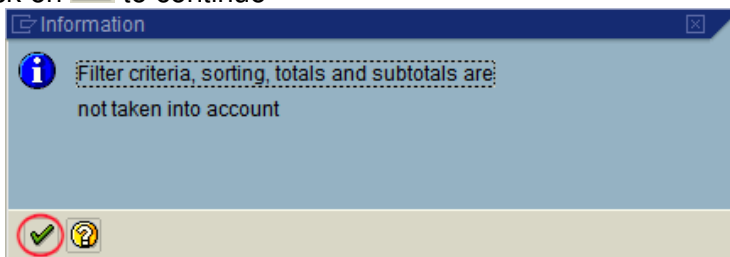
7. To download the results to Excel, Click on List > Export > Spreadsheet




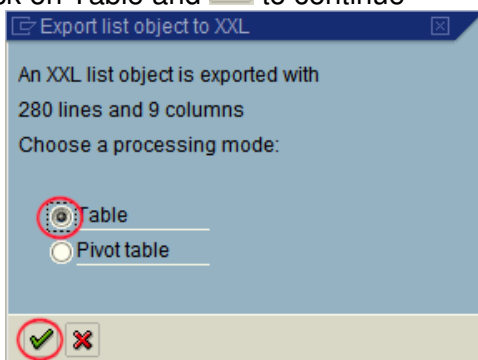
8. Choose All Available Formats → Excel (In Existing XXL Format) and Click on  to continue



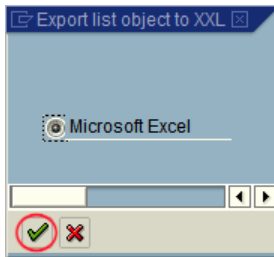
9. Click on  to continue



10. Click on Table and  to continue



11. Click on  to continue

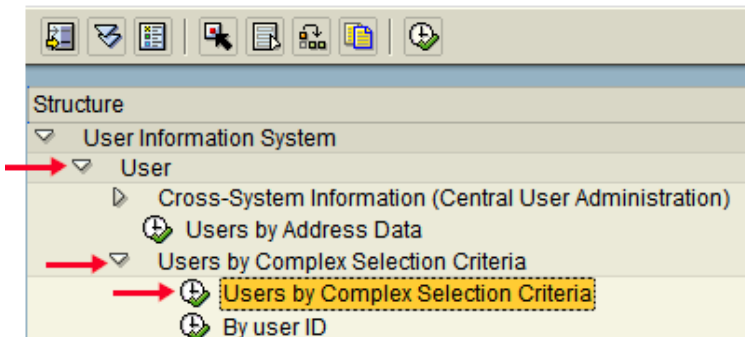


12. Excel will open and display the data.
13. Save the spreadsheet on your computer.

Display Role Assignments for all Users (SUIM)

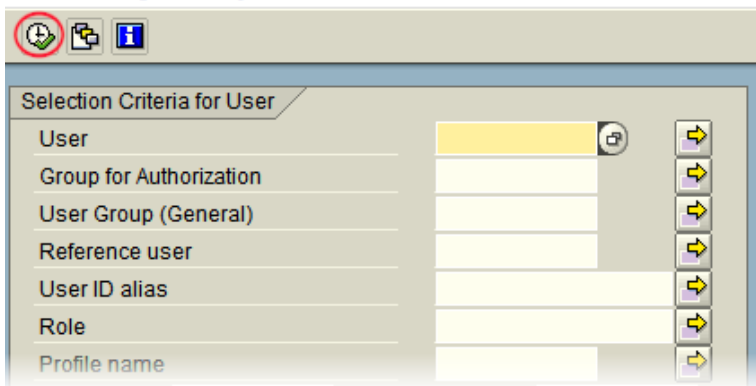
1. Enter transaction SUIM
2. From the User Information System screen, drill down to User > Users by Complex Selection Criteria
 - > Users by Complex Selection Criteria and click on


User Information System











3. Leave all fields blank and click on to execute the report

Users by Complex Selection Criteria






- The list returned should contain all UserID within the agency. Click on the  Roles (Roles) button to display all roles assigned to the user.

Users by Complex Selection Criteria


Roles Profiles Change documents        

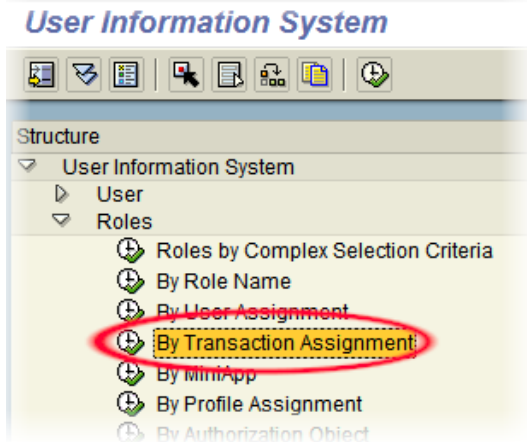
Number of Users Selected: 157


| User Name | Complete name | User group | Account no. | Locked | Valid from | Valid through |
|-----------|----------------|------------|-------------|---|------------|---------------|
| 00000001 | R. J. Jaramola | | | | | |
| 11111111 | First Last | | | | | |
| 11111112 | John Doe | | | | | |
| AL100001 | Alison Farrell | | | | | |
| AL100002 | Alison Farrell | BW | | | | |
| AL100003 | Alison Farrell | ROLLED_OFF | |  | | |
| AL100004 | Alison Farrell | ROLLED_OFF | |  | | |
| AL100005 | Alison Farrell | BW | | | | |
| AL100006 | Alison Farrell | ROLLED_OFF | |  | | |

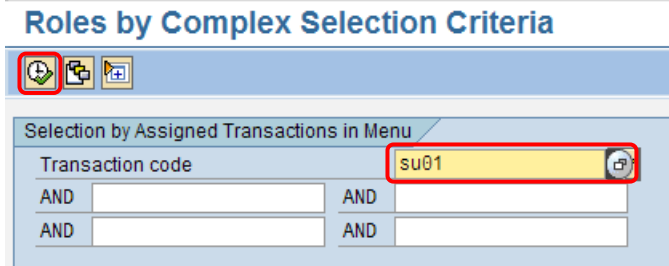
- The report will be displayed. To download the results to Excel see the steps 7 – 13 in the Display Users by Role above.

Display Transactions by Role (SUIM)

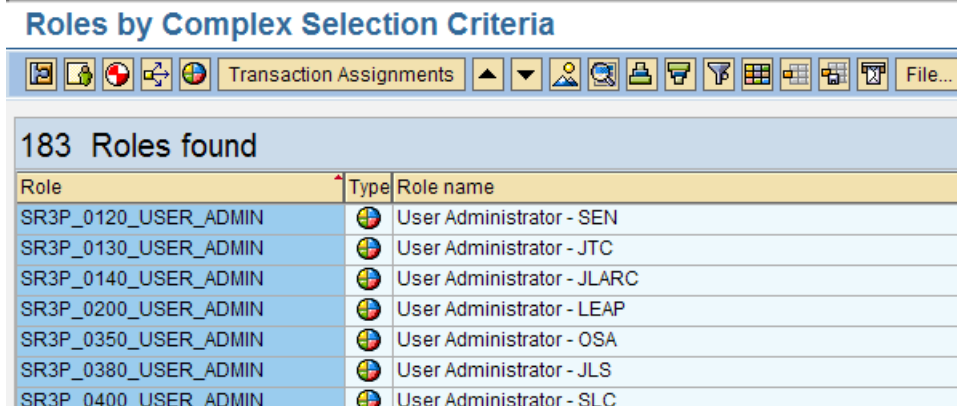
1. Enter transaction 'SUIM' (/nSUIM) to Display Transactions by Role
2. From the User Information System screen, drill down to Roles > By Transaction Assignment and click on  to Execute.










3. Enter the transaction (or search if you don't know it) and click on  to Execute.
NOTE: Single or multiple transactions can be entered here.



4. A list of Transactions by Roles will be generated.
NOTE: You can view User Assignment by selecting a role and the User assignment button.



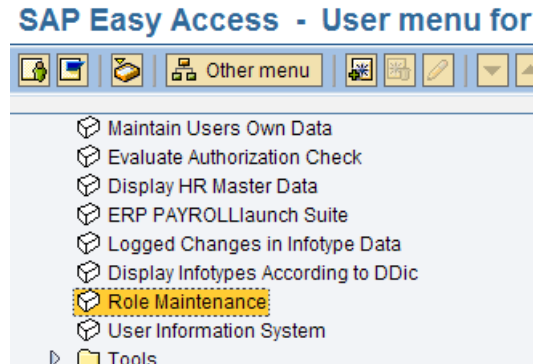
The screenshot shows the 'Roles by Complex Selection Criteria' results screen. It displays a table of 183 roles found. The table has three columns: Role, Type, and Role name. The roles listed are all 'User Administrator' roles with different suffixes.


| Role | Type | Role name |
|----------------------|---|----------------------------|
| SR3P_0120_USER_ADMIN |  | User Administrator - SEN |
| SR3P_0130_USER_ADMIN |  | User Administrator - JTC |
| SR3P_0140_USER_ADMIN |  | User Administrator - JLARC |
| SR3P_0200_USER_ADMIN |  | User Administrator - LEAP |
| SR3P_0350_USER_ADMIN |  | User Administrator - OSA |
| SR3P_0380_USER_ADMIN |  | User Administrator - JLS |
| SR3P_0400_USER_ADMIN |  | User Administrator - SLC |

Display Role Information (PFCG)

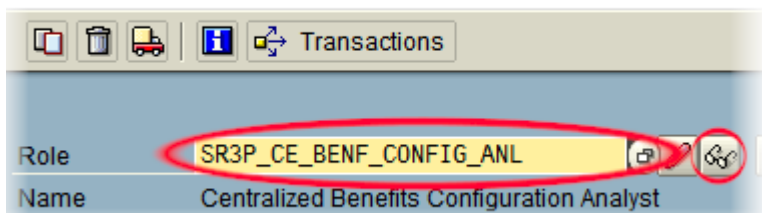
NOTE: To see transaction codes in the User Menu click on Extras → Settings, check the Display Technical Names check box and click the green checkmark button.

1. Enter transaction 'PFCG' (n/PCFG) or select 'Role Maintenance' from the main menu.



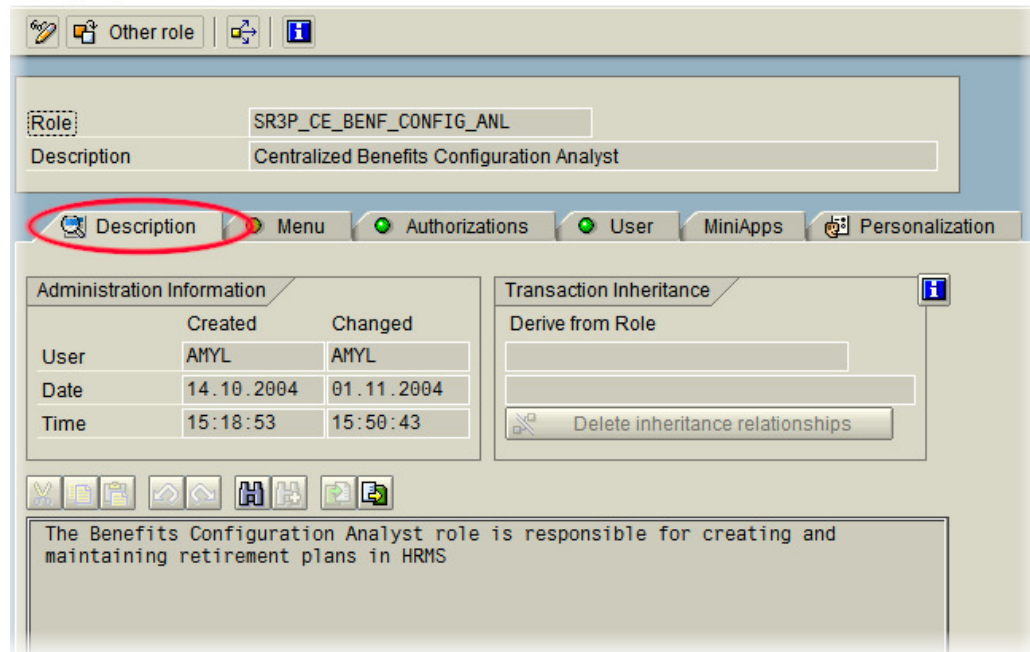
2. Enter the Role Name (or search for possible values) and click on  to Display


Role Maintenance







3. The first tab is Description; it will list who created it, last changed and a description.

Display Roles








4. The second tab is Menu; this shows transactions available via the menu system for this role.
- NOTE:** To see transaction codes in this view click on the 'Switch on technical names'  button.

Display Roles

  Other role  

Role: SR3P_CE_BENF_CONFIG_ANL
Description: Centralized Benefits Configuration Analyst


Description **Menu** Authorizations User MiniApps Personalization


    

Role menu





- Display Spool Requests
- Evaluate Authorization Check
- Maintain Users Own Data
- Display HR Master Data
- Maintain HR Master Data
- Enrollment
- Termination of Participation
- Participation Monitor
- Benefits Participation Overview
- Automatic Plan Enrollment
- EOI Monitor

Target System

 No destination

5. The third tab is Authorizations: this additional information about the authorizations for the role. Click on  to Display Authorization Data for the role.

Display Roles

  Other role  

Role: SR3P_CE_BENF_CONFIG_ANL
Description: Centralized Benefits Configuration Analyst

Description Menu **Authorizations** User MiniApps Personalization

Created by

| | |
|------|------------|
| User | AMYL |
| Date | 14.10.2004 |
| Time | 15:18:53 |


Last Changed On/By


| | |
|------|------------|
| User | AMYL |
| Date | 01.11.2004 |
| Time | 15:40:26 |

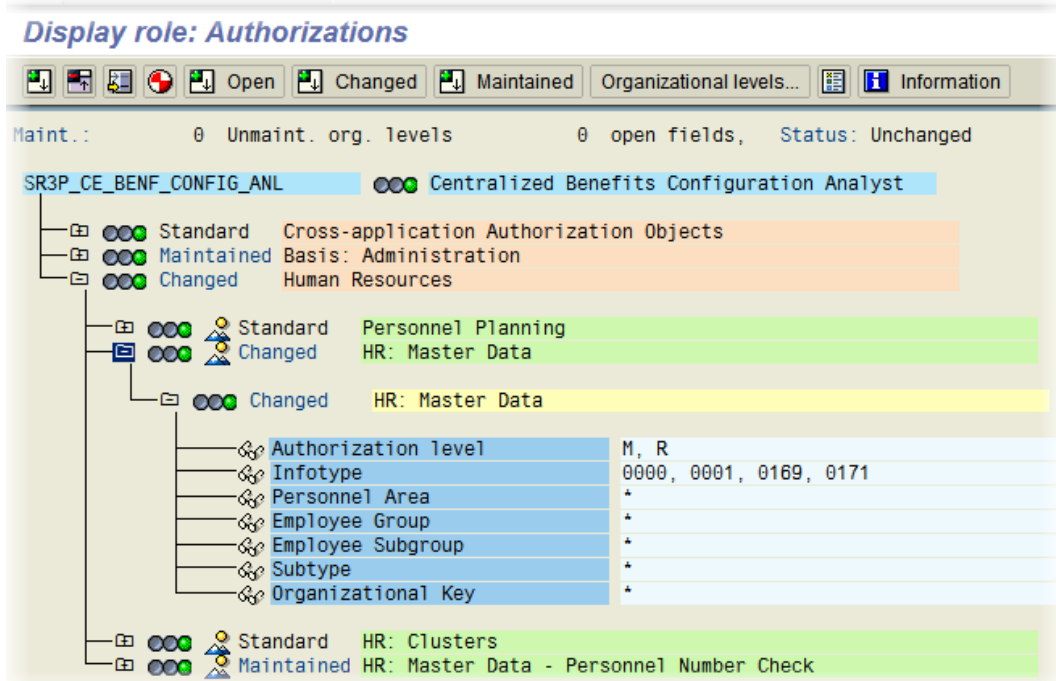
Information About Authorization Profile

| | |
|--------------|--|
| Profile Name | WACBECFGAN |
| Profile Text | Profile for role SR3P_CE_BENF_CONFIG_ANL |
| Status | Authorization profile is generated |

Maintain Authorization Data and Generate Profiles

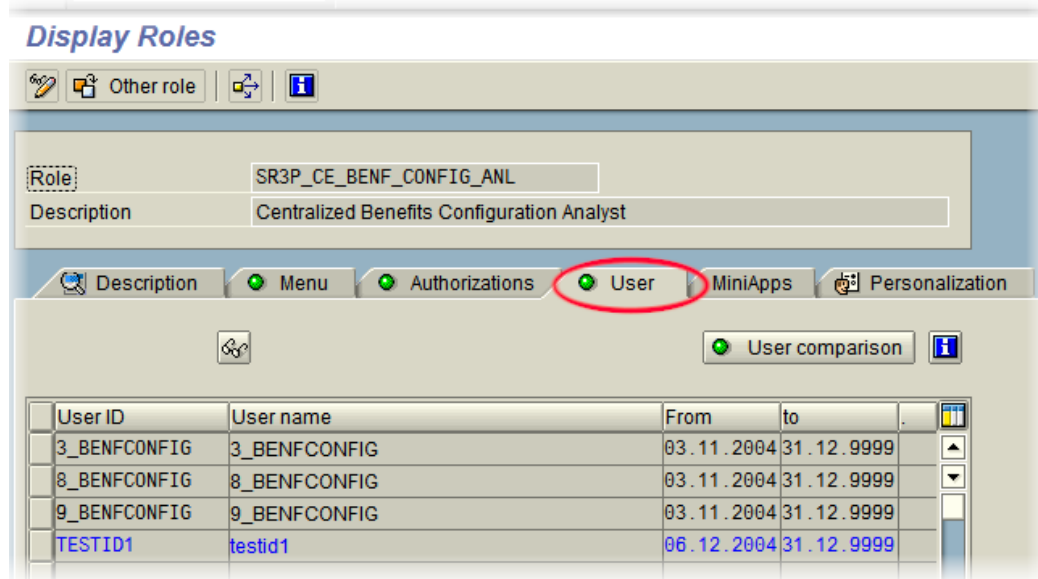
 Display Authorization Data

6. In the Display role: Authorizations screen, expand the node to view specific authorizations. When finished, click on Back(F3)  to return to the Display Roles screen.



7. The fourth tab is User; this will list users assigned to the role. Direct assignments are noted in Black, Indirect (position based) assignments are shown in Blue.

NOTE: The roles should always be assigned to positions.

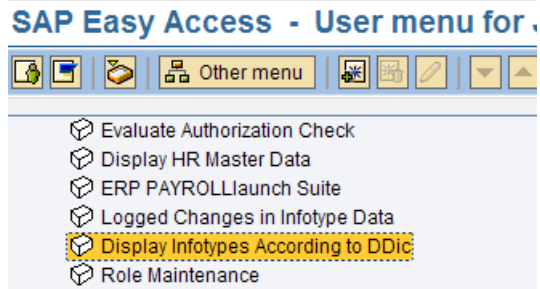


8. The fifth tab is MiniApps and the sixth tab is Personalization. At this time, disregard these tabs.

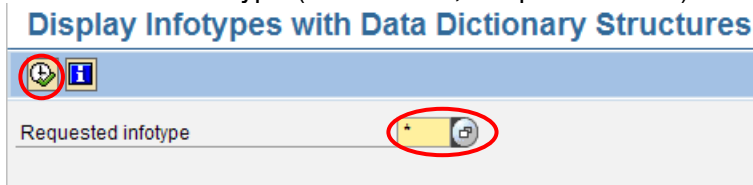


Display List of Infotypes (S_ALR_87101323)

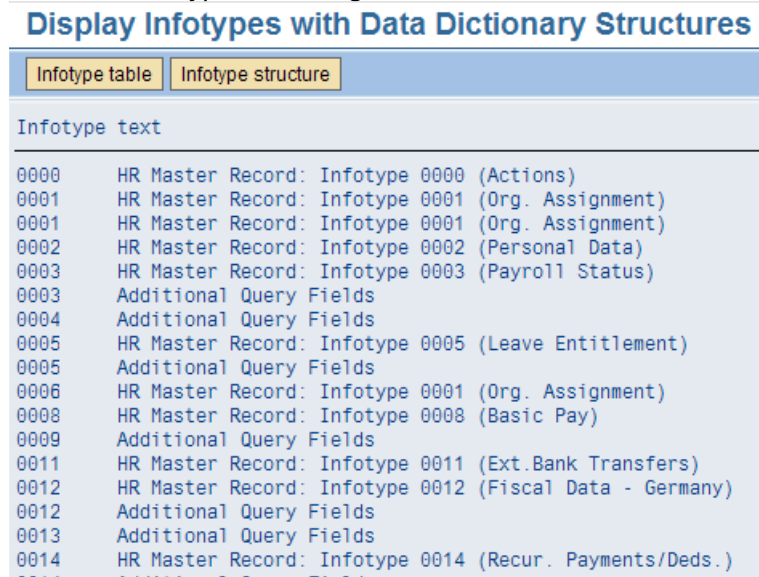
1. Enter transaction 'S_ALR_87101323' (n/S_ALR_87101323) or select 'Display Infotypes According to DDic' from the main menu.



2. Enter the Info Type (* to view all, or specific value) and click on  to Execute.



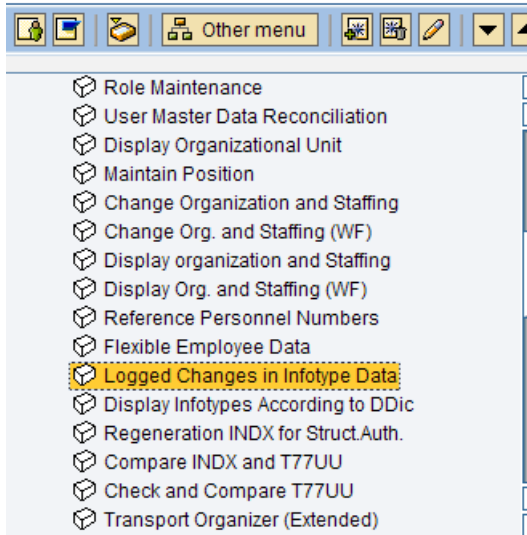
3. A list of Info Types will be generated.



Display Changes in Infotype Data (S_AHR_61016380)

1. Enter transaction 'S_AHR_61016380' (n/S_AHR_61016380) or select 'Logged Changes in Infotype Data' from the main menu.

SAP Easy Access - User menu for



2. Select Long-term documents and enter InfoType to search on and click on  to Execute. Additionally, you can enter a range of InfoTypes and Changed dates.

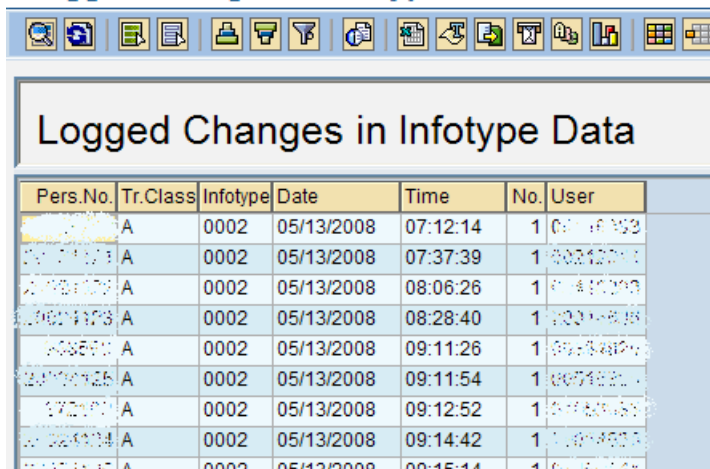
Logged Changes in Infotype Data

The screenshot shows the 'Logged Changes in Infotype Data' SAP transaction screen. The screen is divided into several sections:

- Read documents from database:** Contains checkboxes for 'Long-term documents' (checked) and 'Short-term documents' (unchecked).
- Selection:** Contains a 'Transaction class' section with radio buttons for 'Master data' (selected), 'Appl.data', and 'All'. Below this are input fields for 'Personnel number', 'Infotype' (with value '0002'), 'Changed on', and 'Changed by', each followed by a 'to' field and a selection icon.
- Output options:** Contains a 'Default currency' field and checkboxes for 'Direct output of docs', 'Output program selections', 'New page per doc.', and 'Output in ALV' (checked).
- Sort order:** Contains radio buttons for 'Time' (selected), 'Personnel no.', 'Infotype', and 'User'.

3. A list of Changes in Infotype Data will be generated.

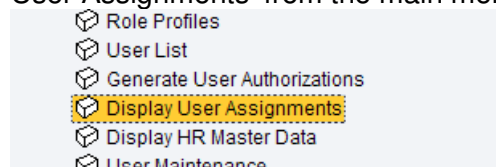
Logged Changes in Infotype Data





| Pers.No. | Tr.Class | Infotype | Date | Time | No. | User |
|----------|----------|----------|------------|----------|-----|----------|
| 11111111 | A | 0002 | 05/13/2008 | 07:12:14 | 1 | 00000000 |
| 11111111 | A | 0002 | 05/13/2008 | 07:37:39 | 1 | 00012345 |
| 11111111 | A | 0002 | 05/13/2008 | 08:06:26 | 1 | 00012345 |
| 11111111 | A | 0002 | 05/13/2008 | 08:28:40 | 1 | 00012345 |
| 11111111 | A | 0002 | 05/13/2008 | 09:11:26 | 1 | 00012345 |
| 11111111 | A | 0002 | 05/13/2008 | 09:11:54 | 1 | 00012345 |
| 11111111 | A | 0002 | 05/13/2008 | 09:12:52 | 1 | 00012345 |
| 11111111 | A | 0002 | 05/13/2008 | 09:14:42 | 1 | 00012345 |
| 11111111 | A | 0002 | 05/13/2008 | 09:15:14 | 1 | 00012345 |




Display User Assignments (ZAUTH_DSP_USR_ASSIGN)

1. Enter transaction 'ZAUTH_DSP_USR_ASSIGN' (/nZAUTH_DSP_USR_ASSIGN) or select 'Display User Assignments' from the main menu.



2. Display Roles and Profiles assigned to User
 - a. Enter the UserID into the 'User Name' field. The UserID should be the user's Personnel Number, **including** leading zeroes. In this example it is '11111111'. To search for the User, click on  to search and select the User.
 - b. Select Roles and Standard Profiles
 - c. Select P_ORIGIN (HR: Master Data)
 - d. Click on  to Execute.

Display User Assignments

d.   Display Authorization Switch  Assigned Persons (Infotype 0105)

User

User Name **a.** 11111111

Assignments

☐ Related Organizational Units

☐ Structural Profiles

b. ☒ Roles and Standard Profiles

☐ Display HR Authorizations

c. ☒ P_ORGIN (HR: Master Data)

☐ P_ORGXX (HR: Master Data - Extended Check)

☐ P_ORGINCON (HR: Master Data with Context)

☐ P_ORGXXCON (HR: Master Data - Extended Check with Context)

☐ P_PERNR (HR: Master Data - Personnel Number Check)

☐ P_ABAP (HR: Reporting)

☐ PLOG (Personnel Planning)




e. The report will display Roles and Profiles assigned to the User selected.

Display User Assignments





Roles and StandardProfiles

User Name 11111111

| | Role | Profile | Start date | End Date |
|--|------------------------|------------|------------|------------|
| Related Roles in OM (Relationship 007) | | | | |
| Standard Profiles in OM (IT 1016) | | | | |
| Roles in User MasterRec | SR3P_DE_PAY_INQ | | 07/08/2009 | 12/31/9999 |
| | SR3P_DE_PERS_ADMIN_INQ | | 07/08/2009 | 12/31/9999 |
| | SR3P_DE_T&A_INQ | | 07/08/2009 | 12/31/9999 |
| Standard Profiles in UserMastRec | | WADPADMINQ | | |
| | | WADPAYINQ_ | | |
| | | WADT&AINQ_ | | |

3. Click the Back button  to go back to previous screen.
4. Display HR Authorizations by Authorization Object
 - a. Enter the UserID into the 'User Name' field. The UserID should be the user's Personnel Number, **including** leading zeroes. In this example it is '11111111'. To search for the User, click on  to search and select the User.
 - b. Select Display HR Authorizations
 - c. Select P_ORGIN (HR: Master Data)
 - d. Click on  to Execute.

Display User Assignments

d.    Display Authorization Switch  Assigned Persons (Infotype 0105)

User

User Name **a.** 11111111

Assignments

☐ Related Organizational Units

☐ Structural Profiles

☐ Roles and Standard Profiles

b. ☒ **c.** Display HR Authorizations

☒ P_ORGIN (HR: Master Data)

☐ P_ORGXX (HR: Master Data - Extended Check)

☐ P_ORGINCON (HR: Master Data with Context)

☐ P_ORGXXCON (HR: Master Data - Extended Check with Context)















☐ P_PERNR (HR: Master Data - Personnel Number Check)

☐ P_ABAP (HR: Reporting)

☐ PLOG (Personnel Planning)

- e. The report will display authorizations assigned to the User selected.

Display User Assignments

Authorizations by Authorization Object

User Name 11111111

| Object | Authorization | Field Name | Authorization Value | Authorization Value |
|---------|---------------|------------|---------------------|---------------------|
| P_ORGIN | WADPADMIN... | INFTY | 0128 | |
| P_ORGIN | WADPADMIN... | INFTY | 0165 | |
| P_ORGIN | WADPADMIN... | INFTY | 0167 | 0171 |
| P_ORGIN | WADPADMIN... | INFTY | 0207 | 0210 |
| P_ORGIN | WADPADMIN... | INFTY | 0234 | 0236 |
| P_ORGIN | WADPADMIN... | INFTY | 0302 | |

BI (Business Intelligence)
ZS_BI_XXXX_USER_ADMIN

Introduction

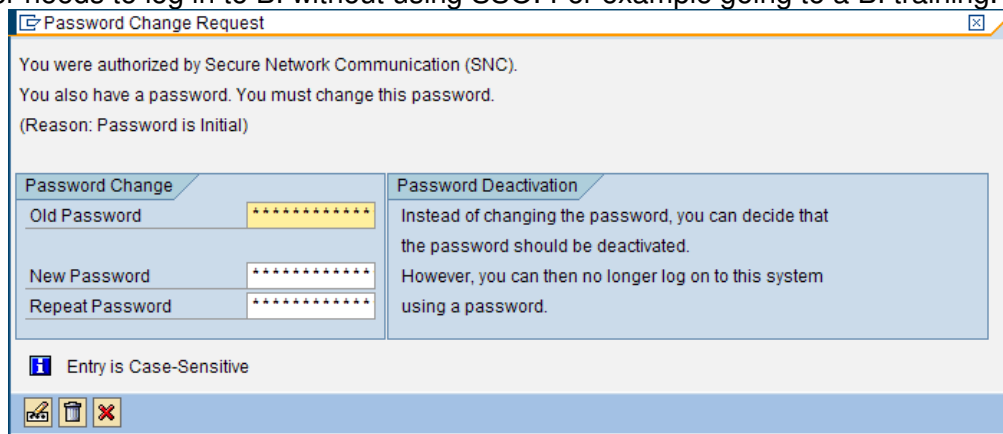
All BI Users must first have an HCM Authorization Profile assigned through the OOSB (Table T77UA). BI UserIDs will have access to retrieve data on the next business day following the creation of their UserID and role assignment(s).

There are two types of BI Reporting Users:

- END_USER: This type of user will retrieve data from BI through the HRMS Portal **or**
- POWER_USER: This type of user will retrieve data directly through BI

BI Users will need UserID & password to display query results on the web (execute WBWT template).

When SSO users login to BI for the first time the system will ask the user to either change the initial password or deactivate it. Our recommendation is **to change the password** and keep a note of it, in case the user needs to log in to BI without using SSO. For example going to a BI training.



The screenshot shows a 'Password Change Request' dialog box. It contains the following text: 'You were authorized by Secure Network Communication (SNC). You also have a password. You must change this password. (Reason: Password is Initial)'. Below this text are two tabs: 'Password Change' and 'Password Deactivation'. The 'Password Change' tab is active and contains three input fields: 'Old Password', 'New Password', and 'Repeat Password', each with a masked password field. The 'Password Deactivation' tab contains the text: 'Instead of changing the password, you can decide that the password should be deactivated. However, you can then no longer log on to this system using a password.' At the bottom of the dialog box, there is a checkbox labeled 'Entry is Case-Sensitive' and a status bar with icons for help, close, and other functions.

NOTE: Changing initial BI password will **not** affect logging in to the portal using SSO with a professional LDAP account. This type of account requires the user to input their network password.

Also, BI UserID accounts are created for:


- Access to E-Recruiting professional roles through the HRMS Portal. This information can be found in the E-Recruiting and HRMS Portal chapters of this handbook.
- Access HCM professional roles through the HRMS Portal with the use of WebGui. Information on how to assign an WebGui group role to the Portal Professional account can be found in the HRMS Portal chapter of this handbook.

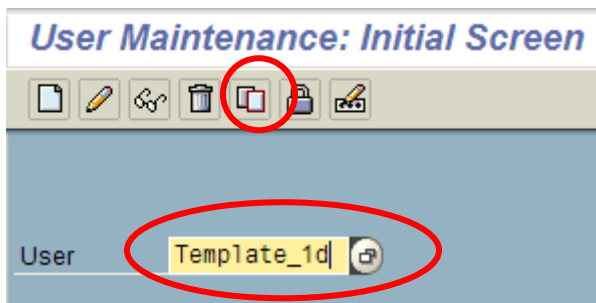
Maintaining a Professional BI UserID Account

Create BI UserID (SU01)


Prerequisites:

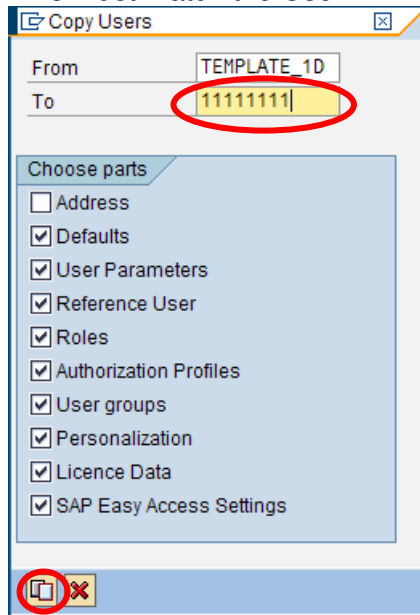
- ✓ UserID is created in HCM, has at least XXXX_Data_Profile role.
- ✓ The Authorization Profile assigned through the OOSB in HCM (not required for E-Recruiting Professional BI Users)

1. Login to the BIP environment (HRMS Business Intelligence);
2. Enter transaction 'SU01' (/nSU01) to create BI UserID
3. Copy the model UserID "Template_1D" to create the new UserID.
 - a. Enter TEMPLATE_1D in the 'User' field.
 - b. Click on  to COPY the Template UserID.

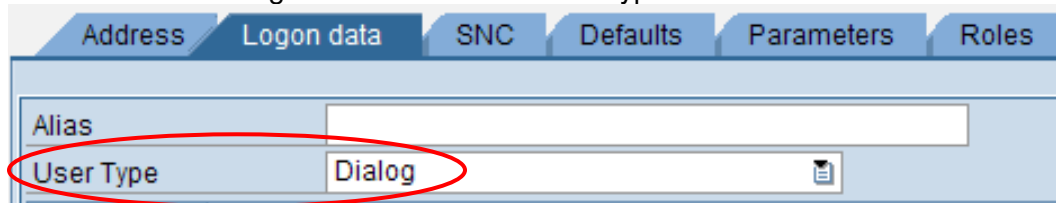


NOTE: The TEMPLATE_1D UserID was created to assist in the creation of new UserIDs. This ID contains basic default settings that all UserIDs will need. There are several fields that will require changes after the copy is performed and before the UserID will be useable in the system.

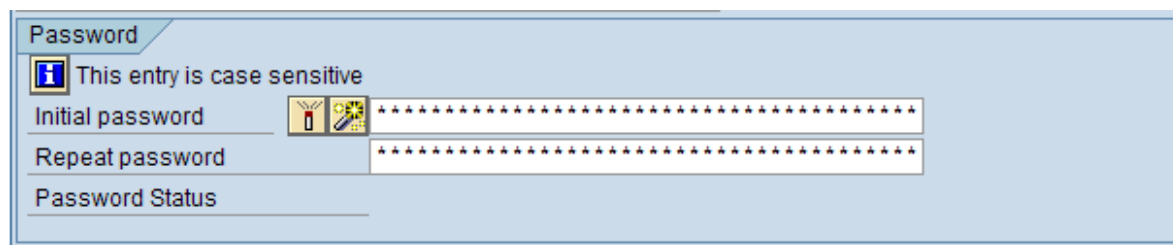
4. Enter the new UserID (Personnel number, **including** leading zeroes to create an eight digit UserID. This must match the UserID in HCM – HRMS Production) and click on  (Copy) to continue.



5. From the 'Logon data' tab, update the following:
a. Make sure Dialog is selected for the User Type





- b. Click in the initial password field and type in an initial password and then retype the same password in the Repeat Password field. Note that 'hardened' password standards apply (i.e. must contain at least 1 letter, 1 number and 1 special character, and must be at least 8 characters long). DO NOT click on the wizard button. This will generate a 40 digit password.



- c. Make note of the password for distribution to the BI User and to map the BI account to the HRMS Portal account if needed.

NOTE: All BI Users will need UserID and password to display query results on the web. The (SSO) BI User should always use the SSO button on the SAP GUI logon pad.






- d. Enter the User Group for your Agency. To search, click on the  button to search for your User Group.

| User Group for Authorization Check | |
|------------------------------------|---|
| User group | WA_1110  |

- e. Enter the valid from and valid through dates.

| Validity Period | |
|-----------------|------------|
| Valid from | 09/10/2008 |
| Valid through | 12/31/9999 |

6. Select the 'Address' tab, enter user's first and last name and any other desired information and press enter when complete.

| Address | | Logon data | SNC | Defaults | Parameters | Roles | Profiles |
|---|---------------------------------------|---|----------------------|---|----------------------|---|----------|
| Person | | | | | | | |
| Title | <input type="text"/> | | | | | | |
| Last name | <input type="text" value="11111111"/> | | | | | | |
| First name | <input type="text"/> | | | | | | |
| Academic Title | <input type="text"/> | | | | | | |
| Format | <input type="text" value="11111111"/> | | | | | | |
| Function | <input type="text"/> | | | | | | |
| Department | <input type="text"/> | | | | | | |
| Room Number | <input type="text"/> | Floor | <input type="text"/> | Building | <input type="text"/> |  | |
| Communication | | | | | | | |
| Language | <input type="text"/> | <input type="button" value="Other communication..."/> | | | | | |
| Telephone | <input type="text"/> | Extension | <input type="text"/> |  | | | |
| Mobile Phone | <input type="text"/> | | |  | | | |
| Fax | <input type="text"/> | Extension | <input type="text"/> |  | | | |
| E-Mail | <input type="text"/> | | | | | | |
| Comm. Meth | <input type="text"/> |  | | | | | |
| <input type="button" value="Assign other company address..."/> <input type="button" value="Assign new company address..."/> | | | | | | | |
| Company | | | | | | | |

7. Click on the 'Defaults' tab. If you did **not** copy this UserID from 'Template_1D', ensure the following fields are filled as shown:

| Address | | Logon data | | SNC | | Defaults | | Parameters | | Roles | | Profiles | |
|--|--|------------------------------------|--|-----|--|----------|--|------------|--|-------|--|----------|--|
| Start menu | | | | | | | | | | | | | |
| Logon Language | | EN | | | | | | | | | | | |
| Decimal Notation | | 1,234,567.89 | | | | | | | | | | | |
| Date Format | | MM/DD/YYYY | | | | | | | | | | | |
| Time Format (12/24h) | | 24 Hour Format (Example: 12:05:10) | | | | | | | | | | | |
| Spool Control | | | | | | | | | | | | | |
| OutputDevice | | LOCL | | | | | | | | | | | |
| <input type="checkbox"/> Output Immediately | | | | | | | | | | | | | |
| <input type="checkbox"/> Delete After Output | | | | | | | | | | | | | |
| Personal Time Zone | | | | | | | | | | | | | |
| of the User | | PST | | | | | | | | | | | |
| Sys. Time Zone | | PST | | | | | | | | | | | |
| CATT | | | | | | | | | | | | | |
| <input type="checkbox"/> Check Indicator | | | | | | | | | | | | | |

If **NOT** using Single Sign On (SSO) you are done. If you **ARE** using SSO continue to step 8.

Single Sign On

8. Click the "SNC" tab. Enter the SNC name in the following format 'p:xxx\yyyy' (see example below).
 - xxx = 3 letter agency code
 - yyyy = user network id

The screenshot shows a web interface with tabs: Address, Logon data, SNC, Defaults, Parameters, Roles, and Profiles. The 'SNC' tab is selected. Under 'SNC Status', there is a green checkmark icon and the text 'SNC is active on this application server', and a red warning icon with the text 'Unsecure logon is allowed (snc/accept_insecure_gui)'. Under 'SNC data', the 'SNC name' field is highlighted with a red circle and contains the text 'p:dop\willw'. Below this field, there is a red warning icon with the text 'Canonical name not determined' and a checkbox labeled 'Unsecure communication permitted (user-specific)' which is currently unchecked.

9. If the update is successful, a green check mark and the message "Canonical name determined" will appear as it does below.

The screenshot shows the same web interface as before, but now the 'SNC name' field contains 'p:dop\willw'. Below this field, there is a green checkmark icon and the text 'Canonical name determined'. The checkbox 'Unsecure communication permitted (user-specific)' remains unchecked.

10. Click on  (Save) when finished.

Assign Professional Roles to a BI UserID Account (SU01)

NOTE: The *GENERAL ACCESS* role *MUST* be assigned to all BI user accounts. For E-Recruiting Professional BI Users this is the only role needed in BI. For assigning multiple users, Mass UserID Maintenance (SU10) can also be used.

Roles for BI UserIDs



BI users will need the following roles:

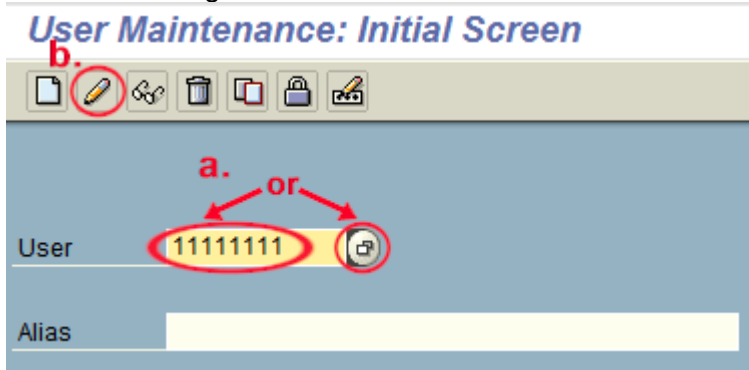
- ZS_BI_GENERAL_ACCESS (Contains general use transactions),
- ZS_BI_XXXX_END_USER **or**
- ZS_BI_XXXX_POWER_USER (where 'XXXX' is your personnel area)
- ZS_BI_XXXX_WBWT Agency Workbook/Web template)
- ZS_BI_SOW_WBWT (State of Washington Workbook/Web template)


and one OR more of the following

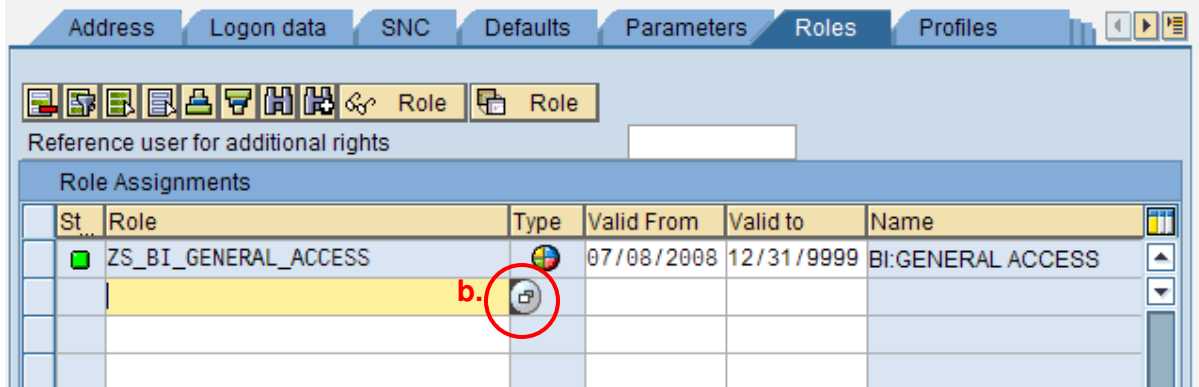
- ZS_BI-FI_ANALYSIS (Access to Financial data)
- ZS_BI-HR_ANALYSIS (Access to HR data)
- ZS_BI-ER_ANALYSIS (Access to E-Recruiting data)
- ZS_BI-GR_ANALYSIS (Access to Grievance data)


Roles in BI are assigned directly to the UserID.

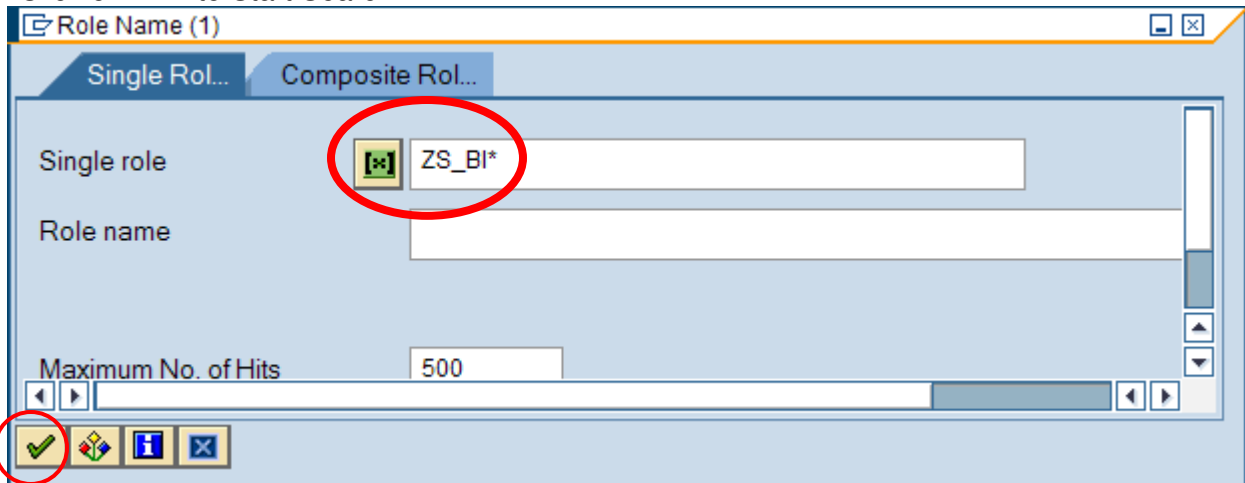
1. Log into BIP (HRMS Business Intelligence);
2. Enter transaction '**SU01**' (/nSU01) to Assign Role(s) to UserID(s)
3. Enter/Search for the UserID.
 - a. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field. In this example it is '11111111'. To search for the User, click on  to search and select the User.
 - b. Click the 'Change'  button.




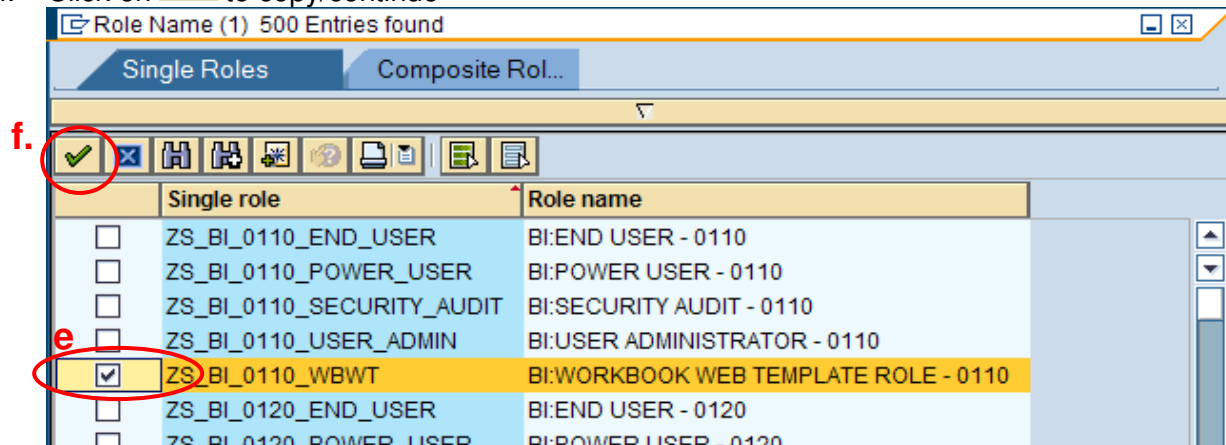
3. Click the 'Roles' tab, enter the Role name.
 - a. If you know the role, type it in the first empty cell and press enter.
 - b. To search for the Role, click on  to search.



- c. Enter ZS_BI* in the 'Single Role' field
- d. Click on  to Start Search





- e. Select the role(s) desired and place a checkmark in the box to the left.
- f. Click on  to copy/continue

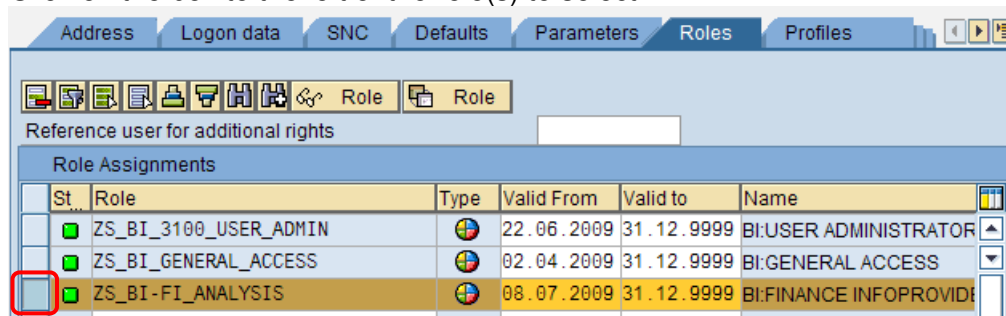





- g. Repeat as necessary to add any additional roles.

1. Close the Display Role screen.
2. Repeat from step 4 for any other roles.

Delete Professional Roles from a BI UserID Account (SU01)

1. Log in to BIP (HRMS Business Intelligence)
2. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field.
3. Click on the Display button , and verify the user.
4. On the Roles tab; Click on Display/Change button  to enter the edit mode.
5. Click on the box to the left of the role(s) to select



| St... | Role | Type | Valid From | Valid to | Name |
|--------------------------|-----------------------|---|------------|------------|------------------------|
| <input type="checkbox"/> | ZS_BI_3100_USER_ADMIN |  | 22.06.2009 | 31.12.9999 | BI:USER ADMINISTRATOR |
| <input type="checkbox"/> | ZS_BI_GENERAL_ACCESS |  | 02.04.2009 | 31.12.9999 | BI:GENERAL ACCESS |
| <input type="checkbox"/> | ZS_BI-FI_ANALYSIS |  | 08.07.2009 | 31.12.9999 | BI:FINANCE INFOPROVIDE |

6. Click on Delete Row  button to delete the role(s)
7. Click the Save  button to save the account.

BI UserID Maintenance

For the complete steps of maintenance processes, refer to the previous chapter HCM UserID Maintenance. The steps are the same in BI as they are in HCM.

[Reset BI Password \(SU01\)](#)

[Lock/Unlock BI UserID \(SU01\)](#)





[Mass BI UserID Lock/Unlock \(SU10\)](#)

Some of the options where the SU10 Mass User Maintenance transaction might be more effective than one-at-a-time changes are:

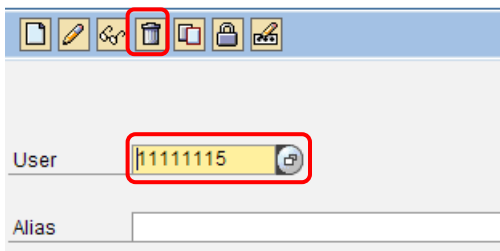
- locking of UserIDs,
- changing Parameters and/or Defaults,
- assigning common roles to a large group

Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):

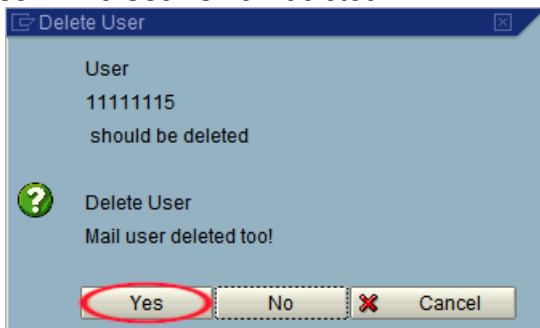
BI:

1. Log into BIP – Business Intelligence Production – through the SAP Logon Pad
2. Enter transaction '**SU01**' (/nSU01) to delete the UserID.
3. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field. In this example it is '11111115'. To search for the User, click on  to search and select the User.
4. Click the Display button  to verify the user
5. Click on the Back button  to go back to the User Maintenance screen
6. Click the  'Delete' button

User Maintenance: Initial Screen





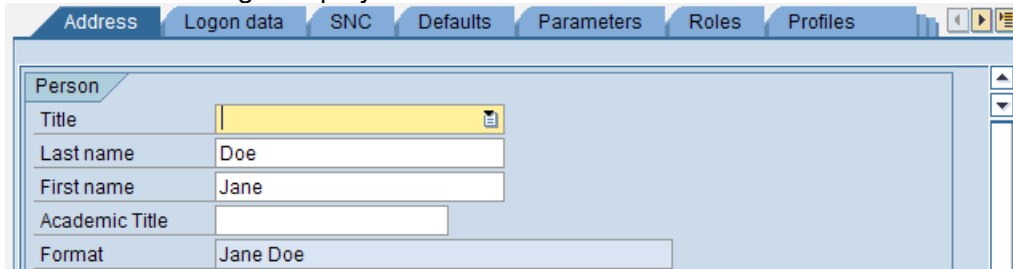
7. A screen like the one below will appear. Click the 'Yes' button if you are sure you want to delete the User. The User is now deleted.



Employee has a Name Change

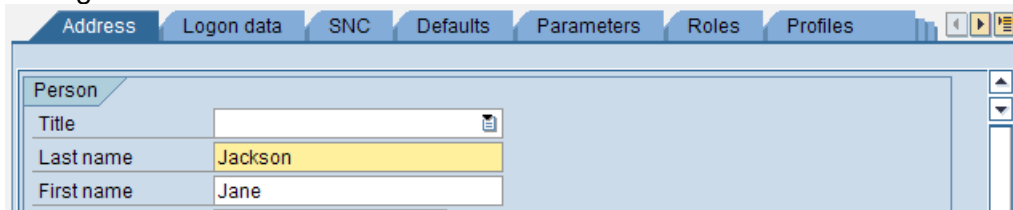
NOTE: When an employee has a name change and the HCM personnel master record is updated, this change does not update the UserID account (SU01) for that employee in BI. The Agency User Administrator must manually go into SU01 and change employee's name.

1. Enter transaction SU01
2. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field
3. Click the Display button  to verify the user
4. Click on the Change/Display button  to enter the edit mode



The screenshot shows the SU01 user display screen. At the top, there are tabs: Address, Logon data, SNC, Defaults, Parameters, Roles, and Profiles. Below the tabs is a 'Person' section with the following fields: Title (empty), Last name (Doe), First name (Jane), Academic Title (empty), and Format (Jane Doe). The 'Last name' field is highlighted in yellow.

5. Change Last and/or First name



The screenshot shows the SU01 user edit screen. At the top, there are tabs: Address, Logon data, SNC, Defaults, Parameters, Roles, and Profiles. Below the tabs is a 'Person' section with the following fields: Title (empty), Last name (Jackson), First name (Jane), Academic Title (empty), and Format (Jane Doe). The 'Last name' field is highlighted in yellow.

6. Click on Save  to save the account.

E-Recruiting User Administrator SERP_USER_ADMIN

Introduction

This will assist/direct you in the administration and maintenance of **E-Recruiting** UserIDs, to ensure all employees have access to E-Recruiting functionality.

State employees will have both an Employee Self Service (ESS) account and an E-Recruiting account. Employees may access E-Recruiting from their ESS account (My Career tab). This tab allows the state employee to search and apply for jobs through E-Recruiting.

Employees will be able to reset their own password for ESS as long as they have entered their email address in their ESS personal information.

If the password for the ESS account needs resetting, you will perform this action accessing the UserID (personnel number) account in the HRMS Portal. If the email address has been added in ESS the employee will receive an email with their reset password. **NOTE:** *This functionality is not supported on the new IE8 browser.*

If the password for the E-Recruiting account needs resetting, you will perform this action accessing the UserID (personnel number) account in EP0 through the SAPGUI Logon Pad.

There will also be agency Recruiters that will need access to E-Recruiting through the HRMS Portal. Agency Recruiters WILL NOT access E-Recruiting through their ESS accounts but through a different account in the HRMS Portal. We call this a Professional Portal account. This professional account will allow agency recruiters to perform recruiter functions through E-Recruiting. The professional user can also run E-Recruiting reports if assigned the appropriate roles in EP0 and in BI.

To have a successful Professional account for E-Recruiting through the HRMS Portal you will first need to make sure all of the appropriate accounts are created. *The accounts that are needed can be found listed in the [Types of E-Recruiting Users](#) section.*

Types of E-Recruiting Users - New to Launch B (October 2008)

- ◆ Internal Job Seeker – This account is a Non-Professional E-Recruiting account created by DOP Centralized Security Administrators in EP0 to give access for internal job seekers to search and apply for jobs through their My Career tab in Employee Self Service (ESS).
- ◆ E-Recruiter – This account is a Professional E-Recruiting account where the user performs a variety of recruitment activities. This type of user needs to have the following accounts created:

1. E-Recruiting roles assigned to the UserID account in EP0.


E-Recruiting professional roles assigned in EP0 should also have a corresponding HRMS Portal Group role assigned to their Professional Portal account. Not all E-Recruiting professional roles have a corresponding portal group role. The available corresponding portal group roles are listed in the crosswalk table below.

| E-Recruiting Roles | Portal Roles |
|--------------------------------|------------------------------|
| SERP_RCF_ASSESSMENT | ER_Assessment_GRP |
| SERP_RCF_DE_ADMIN_LIMITED | ER_DeCentralAdminLimited_GRP |
| SERP_DE_RCF_JOB_SEEKER_SUPPORT | ER_DeCentralJSSupport_GRP |
| SERP_RCF_DECISION_MAKER | ER_DecisionMaker_GRP |
| SERP_RCF_MGR_AS_RECRUITER | ER_ManagerAsRecruiter_GRP |
| SERP_RCF_RECRUITER | ER_Recruiter_GRP |
| SERP_RCF_RECRUITER_LIMITED | ER_RecruiterLimited_GRP |
| SERP_RCF_RECRUITER_SUPPORT | ER_RecruiterSupport_GRP |
| SERP_RCF_REQ_REQUESTER | ER_RequisitionRequest_GRP |

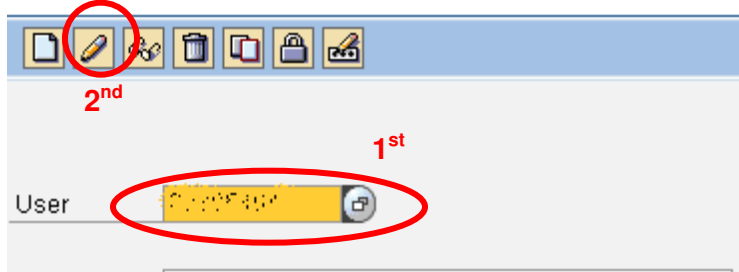
2. Business Intelligence (BI) User Administrator creates UserID account and assigns/verifies the ZS_BI_GENERAL_ACCESS role is assigned in BIP.
3. Professional account in the HRMS Portal. The agency Portal User Administrator checks to see if there is already an LDAP account (email address login account) in the HRMS Portal. If not, then the user administrator creates an agency domain\network username account (UME: example; dop\juliaw). **AND**
 - Assigns the E-Recruiting portal group roles (corresponding to roles assigned in EP0).
 - Map the professional portal account to the BIP userID account.

Maintaining a Professional E-Recruiting UserID Account

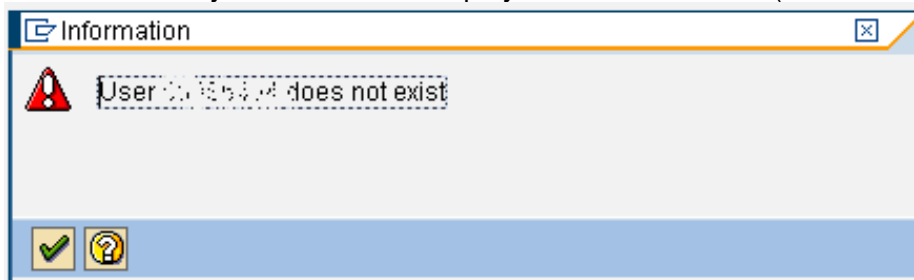
Assign Roles to E-Recruiting UserID's

1. Log into **E-Recruiting EP0** (HRMS E-Recruiting Production), from the SAPGUI logon pad.
2. In the transaction field, enter transaction code **SU01** (/nsu01) to get to User Maintenance to assign a role(s) to a UserID.
3. Enter the UserID (8 digit personnel number, **including** leading zeroes) in to the "User" field, **OR**, click on  to search and select the User. Click the change icon.

User Maintenance: Initial Screen



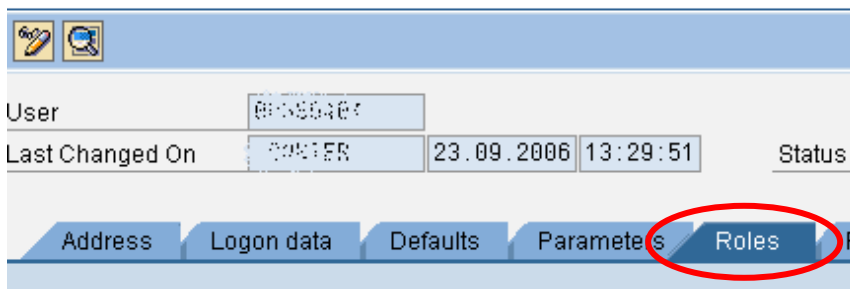
4. If you see the "User xxxxxxxx does not exist" pop-up box, there are a couple of possibilities; either the E-Recruiting UserID has not yet been created, --or-- the UserID you entered is incorrect. Click the green check, then confirm/verify the UserID you entered is correct. If not, repeat step 3 with correct UserID. If you still see this pop-up, you will have to wait until this E-Recruiting UserID has been created by the DOP New Employee UserID Process (HRUSER process).




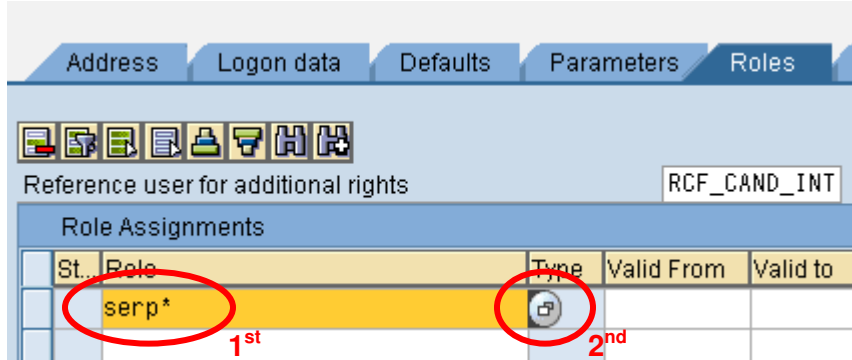
NOTE: If more than a week has elapsed since the new person was entered into the HRMS database and they still haven't appeared in E-Recruiting (or ESS) call the DOP Help desk at 360-664-6400 and ask for assistance from the DOP Central Security Administrators.

5. On the "Maintain User" screen, click the "Roles" tab.

Maintain User



6. Search for the E-Recruiting role to be assigned. Enter “**serp***” in the first empty cell under “Role”, and click on .

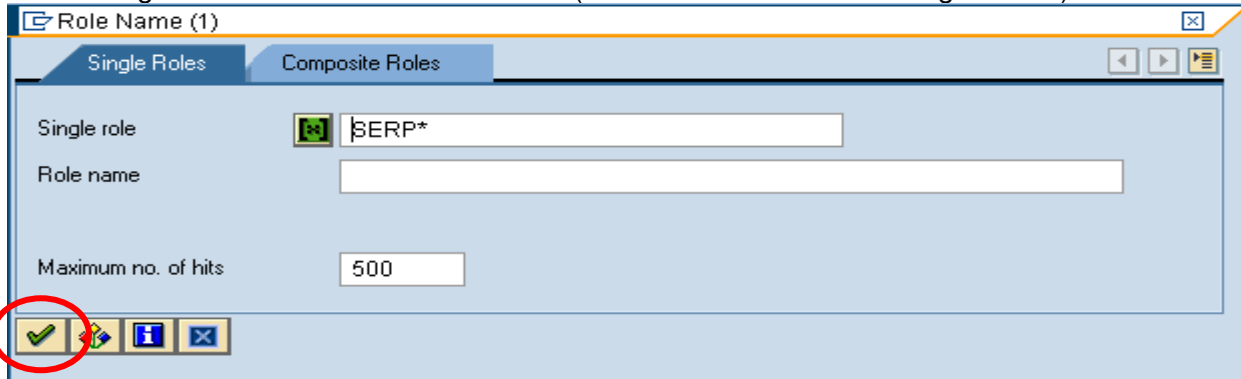


Address Login data Defaults Parameters Roles

Reference user for additional rights: RCF_CAND_INT

| St. | Role | Type | Valid From | Valid to |
|-----|-------|------|------------|----------|
| | serp* | | | |

7. Click the green checkmark to start search. (Make sure the tab is on Single Roles)



Role Name (1)

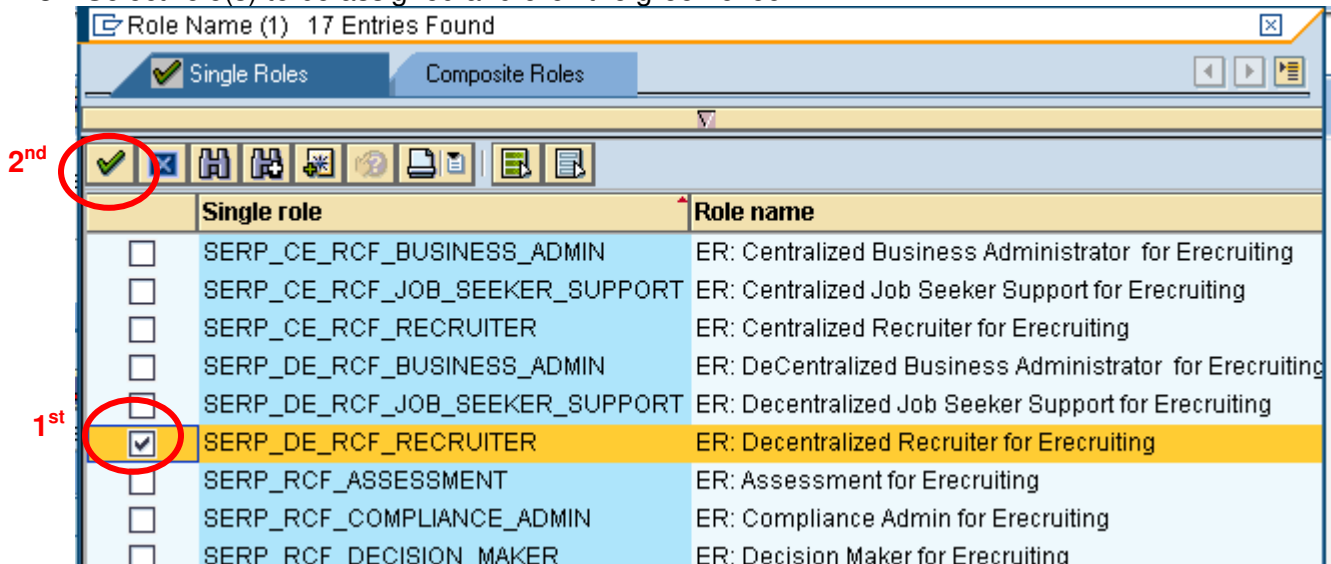
Single Roles Composite Roles

Single role: SERP*

Role name:

Maximum no. of hits: 500


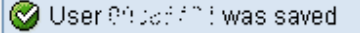
8. Select role(s) to be assigned and click the green check.




Role Name (1) 17 Entries Found

Single Roles Composite Roles

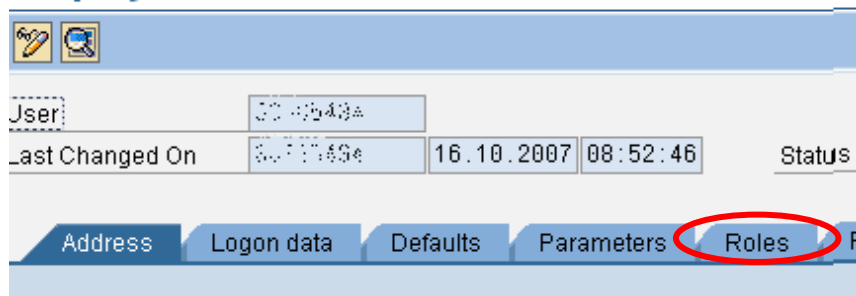
| | Single role | Role name |
|-------------------------------------|--------------------------------|--|
| <input type="checkbox"/> | SERP_CE_RCF_BUSINESS_ADMIN | ER: Centralized Business Administrator for Erecruiting |
| <input type="checkbox"/> | SERP_CE_RCF_JOB_SEEKER_SUPPORT | ER: Centralized Job Seeker Support for Erecruiting |
| <input type="checkbox"/> | SERP_CE_RCF_RECRUITER | ER: Centralized Recruiter for Erecruiting |
| <input type="checkbox"/> | SERP_DE_RCF_BUSINESS_ADMIN | ER: DeCentralized Business Administrator for Erecruiting |
| <input type="checkbox"/> | SERP_DE_RCF_JOB_SEEKER_SUPPORT | ER: Decentralized Job Seeker Support for Erecruiting |
| <input checked="" type="checkbox"/> | SERP_DE_RCF_RECRUITER | ER: Decentralized Recruiter for Erecruiting |
| <input type="checkbox"/> | SERP_RCF_ASSESSMENT | ER: Assessment for Erecruiting |
| <input type="checkbox"/> | SERP_RCF_COMPLIANCE_ADMIN | ER: Compliance Admin for Erecruiting |
| <input type="checkbox"/> | SERP_RCF_DECISION_MAKER | ER: Decision Maker for Erecruiting |

9. Click on  (just right of the transaction box, top of your screen) to save changes; you should see  in the lower left status area of your screen.

Reconciling the Role

10. On the “User Maintenance: Initial Screen”, click  Display.
11. On the “Display User” screen, click the “roles” tab.

Display User




The screenshot shows the 'Display User' screen. At the top, there are fields for 'User' (containing 'RCF_CA') and 'Last Changed On' (containing '16.10.2007 08:52:46'). Below these fields is a tabbed interface with tabs for 'Address', 'Logon data', 'Defaults', 'Parameters', 'Roles', and 'P'. The 'Roles' tab is highlighted with a red circle.

12. Double-click the green icon to the left of the role name you just assigned; the “Display Roles” screen will open in a new window.



The screenshot shows the 'Display Roles' screen. It has tabs for 'Address', 'Logon data', 'Defaults', 'Parameters', and 'R'. Below the tabs is a section titled 'Role Assignments' with a table. The table has columns 'St...', 'Role', 'Type', and 'Valid From'. The first row of the table is highlighted with a red circle, showing a green icon in the 'St...' column, the role name 'SERP_DE_RCF_RECRUITER' in the 'Role' column, a globe icon in the 'Type' column, and the date '23.09.2006' in the 'Valid From' column.

| St... | Role | Type | Valid From |
|---|-----------------------|---|------------|
|  | SERP_DE_RCF_RECRUITER |  | 23.09.2006 |

13. Note the yellow triangle, and click on the “User” tab.

Display Roles

The screenshot shows the 'Display Roles' window. At the top, there are icons for 'Other role', a search icon, and an information icon. Below this, the 'Role' field contains 'SERP_DE_RCF_RECRUITER' and the 'Description' field contains 'ER: Decentralized Recruiter for Erecruiting'. At the bottom, there is a tabbed interface with tabs for 'Description', 'Menu', 'Workflow', 'Authorizations', 'User', and 'MiniApps'. The 'User' tab is highlighted with a yellow triangle and a red circle.

14. Note the red light, and click on the “User comparison” button.

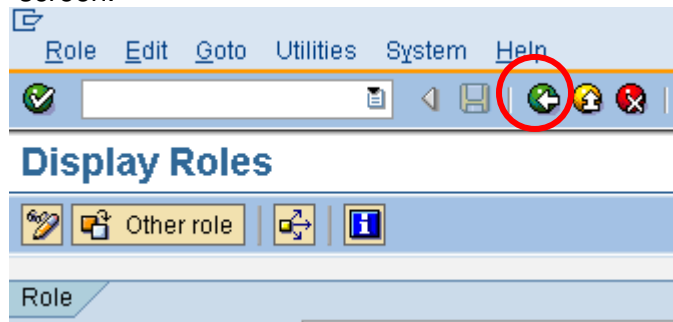
Display Roles

The screenshot shows the 'Display Roles' window. The 'Role' field contains 'SERP_DE_RCF_RECRUITER' and the 'Description' field contains 'ER: Decentralized Recruiter for Erecruiting'. At the bottom, there is a tabbed interface with tabs for 'Description', 'Menu', 'Workflow', 'Authorizations', 'User', and 'MiniApps'. The 'User' tab is highlighted with a yellow triangle. Below the tabs, there is a button labeled 'User comparison' with a red light icon, which is highlighted with a red circle.

15. Click on “Complete comparison”

The screenshot shows the 'Compare Role User Master Record' window. It has two main sections: 'Last comparison' and 'Complete adjustment'. Both sections show the same data: 'User: TONYA', 'Date: 23.09.2006', and 'Time: 14:24:52'. Below these sections, there is a message: 'Information for user master comparison: Status: User assignment has changed since the last user master record comparison'. At the bottom, there is a button labeled 'Complete comparison' with a red light icon, which is highlighted with a red circle.

16. Note the green lights on the “User comparison” button, and on the “User” tab. Click the green “back” arrow to close the window opened in Step #13, and you will return to the “Display User” screen.



17. Click the green “back” arrow and you will return to the User Maintenance screen.

You have just assigned E-Recruiting professional roles in EP0. You will need to contact your agency’s BI User Administrator and Portal User Administrator to create the required accounts to access E-Recruiting through the HRMS Portal. BI account will need the required General_Access role assigned; the professional portal account will need the corresponding E-Recruiting portal group roles assigned.

These procedures can be found in the Business Intelligence and HRMS Portal chapters in this handbook.

E-Recruiting UserID Maintenance

For the complete steps of maintenance processes, refer to the previous chapter HCM UserID Maintenance. The steps are the same in E-Recruiting as they are in HCM.



[Reset ER Password \(SU01\)](#)

[Lock/Unlock ER UserID \(SU01\)](#)

[Mass Lock/Unlock ER UserID \(SU10\)](#)

Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):

E-Recruiting: DO NOT DELETE THESE ACCOUNTS! Delete the roles only


1. Login to E-Recruiting EP0 (HRMS E-Recruiting Production)
2. Enter transaction ‘**SU01**’ (/nSU01) to delete the roles.
3. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the ‘User’ field
4. Click the Display button  to verify the user
5. Click on  to enter Edit mode

- Click on the Roles Tab

| St... | Role | Type | Valid From | Valid to | Name |
|--------------------------|----------------------------|------------------------------|------------|------------|------------------------------|
| <input type="checkbox"/> | SERP_RCF_MGR_AS_RECRUITER | ER: Manager as Recruiter | 10/21/2008 | 12/31/9999 | ER: Manager as Recruiter |
| <input type="checkbox"/> | SERP_RCF_RECRUITER | ER: Recruiter for Erecruitin | 10/21/2008 | 12/31/9999 | ER: Recruiter for Erecruitin |
| <input type="checkbox"/> | SERP_RCF_RECRUITER_SUPPORT | ER: Recruiter Support for E | 10/21/2008 | 12/31/9999 | ER: Recruiter Support for E |

- Click on the box to the left of the role(s) to select

| St... | Role | Type | Valid From | Valid to | Name |
|-------------------------------------|----------------------------|------------------------------|------------|------------|------------------------------|
| <input checked="" type="checkbox"/> | SERP_RCF_MGR_AS_RECRUITER | ER: Manager as Recruiter | 10/21/2008 | 12/31/9999 | ER: Manager as Recruiter |
| <input checked="" type="checkbox"/> | SERP_RCF_RECRUITER | ER: Recruiter for Erecruitin | 10/21/2008 | 12/31/9999 | ER: Recruiter for Erecruitin |
| <input checked="" type="checkbox"/> | SERP_RCF_RECRUITER_SUPPORT | ER: Recruiter Support for E | 10/21/2008 | 12/31/9999 | ER: Recruiter Support for E |

- Click the Delete Row button  to delete the role(s)



| St... | Role | Type | Valid From | Valid to | Name |
|--------------------------|----------------------------|------------------------------|------------|------------|------------------------------|
| <input type="checkbox"/> | SERP_RCF_RECRUITER | ER: Recruiter for Erecruitin | 10/21/2008 | 12/31/9999 | ER: Recruiter for Erecruitin |
| <input type="checkbox"/> | SERP_RCF_RECRUITER_SUPPORT | ER: Recruiter Support for E | 10/21/2008 | 12/31/9999 | ER: Recruiter Support for E |

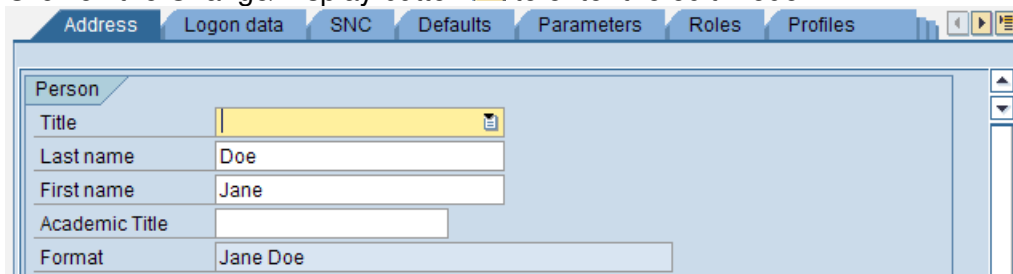
- Click  Save.

NOTE: HCM, BI and Portal User Administrators need to do clean up on these professional user accounts if the users had access to those system

Employee has a Name Change

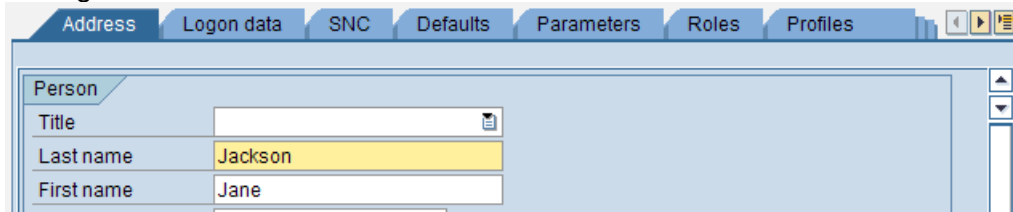
NOTE: When an employee has a name change and the HCM personnel master record is updated, this change does not update the UserID account (SU01) for that employee in E-Recruiting. The Agency User Administrator must manually go into SU01 and change employee's name.

1. Enter transaction SU01
2. Enter the UserID (8 digit Personnel Number, **including** leading zeroes) into the 'User' field
3. Click the Display button  to verify the user
4. Click on the Change/Display button  to enter the edit mode



| Person | |
|----------------|----------|
| Title | |
| Last name | Doe |
| First name | Jane |
| Academic Title | |
| Format | Jane Doe |

5. Change Last and/or First name



| Person | |
|------------|---------|
| Title | |
| Last name | Jackson |
| First name | Jane |

6. Click on Save  to save the account.

HRMS Portal – User Admin

Introduction

There are three types of Portal Logon ID's:

1. Personal ESS User Logon ID - Created by Department of Personnel (DOP). **The Logon ID is the user's 8 digit Personnel Number.** This Logon ID may be locked, unlocked or have its password reset by the Agency's Portal User Administrator(s).
2. Professional LDAP Logon ID - Users accessing the Portal who are connected to the state's Active Directory tree will be granted Portal access based on their email address and network password. **The Logon ID is the user's agency email address.** Password resets for these are the responsibility of the agency network admins.
3. Professional UME Logon ID - Created by the agencies' Portal User Admins. **The Logon ID is the user's agency domain\network username (dop\warrenk).** These accounts require maintenance by the agency User Admins, including creation, deletion, password resetting, locking and unlocking of the accounts, and role/group assignments.

Logon to the HRMS Portal

1. Logon to the HRMS Portal from work; open your web browser and enter this URL if your agency is in the Enterprise Active Directly (*INSIDE* the State Government Network) <https://myhrms.wa.gov/iri>
2. Logon to Portal from work, home or anywhere outside the State Government Network (SGN) enter: <https://wahrms.wa.gov/iri>
 - Inside the SGN (In the Active Directory) - enter your work email address (like warrenk@dis.wa.gov) as your Logon ID to enter the secure (HTTPS) portal. Use your normal network password to login. If the agency is single sign-on (SSO), users should go directly into the portal. (If you are logging in outside of the SGN you would still use your email address and network password).
 - Outside the SGN - If you normally have to log into the Portal using your agency domain\network username (like dis\warrenk) there will be no difference in Logon ID or password from any location.

Professional Portal Accounts

There are two ways to setup access for a user in the Portal. This depends on whether or not your agency is connected to the State Government Active Directory:

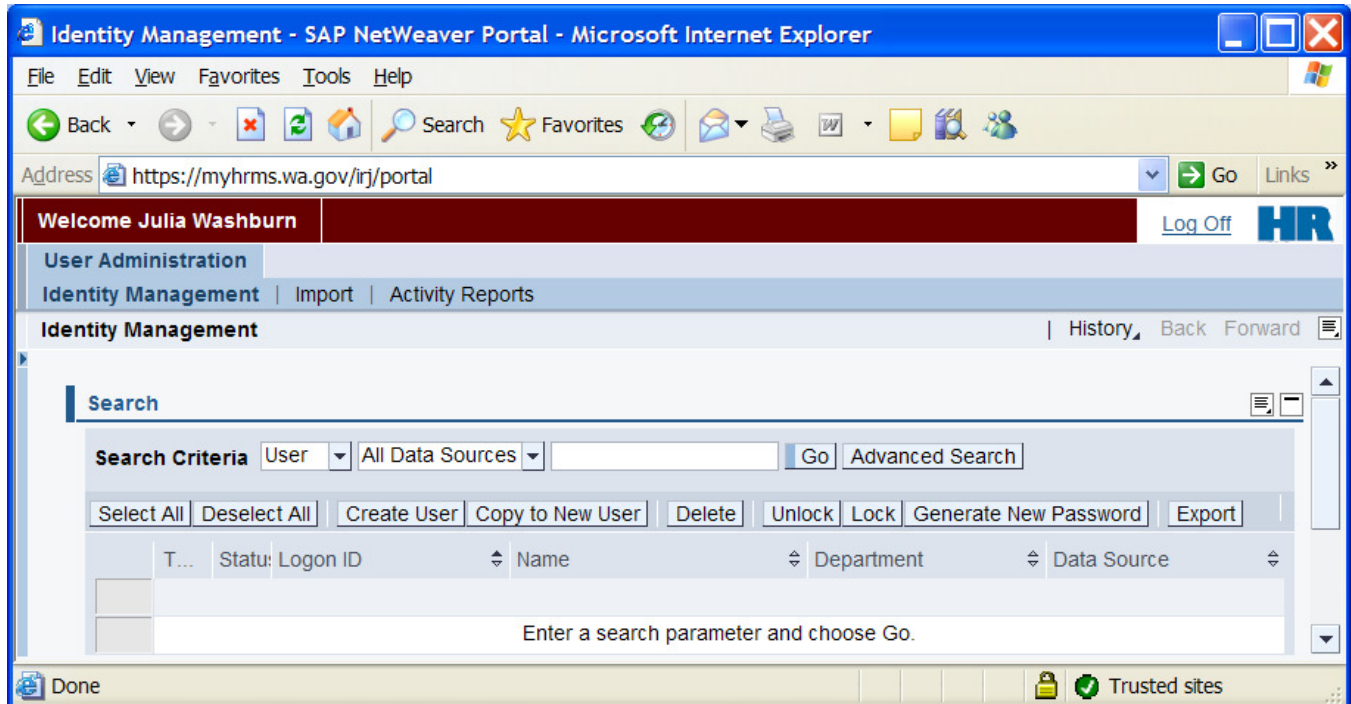
1. If you are IN the State Government Active Directory, your employee's accounts are already created in the portal. The user's email address is his/her Portal Logon ID. Logging into the portal is based on the user's email address and network password and could also possibly be Single Sign On (SSO).
2. If you are NOT a member of the State Government Active Directory, you must Create/Delete your agency Professional Portal UserID/Logon IDs and manage their passwords.

As a Portal User Administrator, you may:

- a. Assign the User Admin SINGLE role. (*User* Admin*)
- b. Assign the HR HtmlGui GRP GROUP role. (Access to HCM through the WEBGUI)
- c. Assign the BI Reports GRP GROUP role. (Access to BI reports and/or E-Recruiting reports)
- d. Assign E-Recruiting GROUP Roles (Access to E-Recruiting functionality)
- e. Map the Portal Logon ID to BIP UserID Account.

The image below shows the HRMS Portal. You should at LEAST have the "User Administration" tab shown, and the "Identity Management" sub-tab also selected. Many actions can be initiated from this screen directly: *Create User, Delete, Lock/Unlock, and Advanced Search*. We recommend using the "Advanced Search" option if you do not know the exact Logon ID.

NOTE: To search for the e-mail address as a Logon ID you have to use the Advanced Search and search by the e-mail field.



Advanced Search

Select the “Advanced Search” option on the Identity Management screen. This will take you to the following screen:

1. Search for a user by the Logon ID, Last Name, First Name or E-Mail Address
Hint: When searching you may substitute the asterisk in any character position to represent unknown characters or wrap known characters around multiple asterisks. (EX: warrenk*; *@*.wa.gov)
2. Click the Search button. You will see the screen similar to the one shown below.

Search

Advanced User Search

☒ Frequently-Used Information
 ☐ General Information
 ☐ Account Information
 ☐ Contact Information
 ☐ Additional Information

Logon ID:
 Last Name:
 First Name:
 E-Mail Address:
 Telephone:
 Fax:
 Mobile:
 Unapproved Users: ☐
 Security Policy:
 Data Source:

| Type | Status | Logon ID | Name | Department | Data Source |
|------|--------|------------------------|---------------------|------------|-------------|
| | | V:\nowebapp\active\CCM | Kelly, Warren (DIS) | | LDAP |
| | | V:\nowebapp\active\CCM | Kelly, Warren (DOP) | HRISD | LDAP |
| | | | | | |
| | | | | | |
| | | | | | |

3. Click on the user you need. The selected user will be highlighted and the Details view will be shown.

Advanced Search can be used to find all types of Portal user accounts: ESS, Professional LDAP (e-mail) and Professional UME (domain\network username)

Maintaining a Professional Portal Logon ID Account

Creating Professional Portal Logon IDs (UME)

NOTE: If you are in the Active Directory and/or a Single Sign On (SSO) agency you do not need to create Professional Portal accounts. They are created automatically and the login ID is the e-mail address. To login to those accounts you will need to use your network password. You will only need to assign groups/roles to those accounts and map to the BI account.

The screenshot shows the 'Advanced User Search' window. At the top, there is a message 'No element found.' and a 'Search' button. Below this, there are three tabs: 'Frequently-Used Information', 'General Information', and 'Account Information'. The 'Frequently-Used Information' tab is selected. It contains several input fields: 'Logon ID' (with 'dop\warren' entered), 'Last Name', 'First Name', 'E-Mail Address', 'Telephone', 'Fax', and 'Mobile'. There are also checkboxes for 'Unapproved Users' and dropdown menus for 'Security Policy' (set to 'All') and 'Data Source' (set to 'All Data Sources'). At the bottom of the form, there are buttons for 'Select All', 'Deselect All', 'Create User' (circled in red), 'Copy to New User', and 'Delete'. Below the buttons is a table with columns for 'Type', 'Status', and 'Logon ID'.

1. Click on the “Create User” button (circled in red above) and your screen format will change to what is shown below:

Details

Save Cancel

General Information

Account Information

Contact Information

Additional Information

Assigned Roles

Assigned Groups

Logon ID: *

DOP\warrenk

☒ Define Initial Password

☐ Generate Password

☐ Disable Password

Define Password: *

••••••••

Confirm Password: *

••••••••

Last Name: *

Kelly

First Name:

Warren

E-Mail Address:

Form of Address:

Language:

Activate Accessibility Feature:

☐

Security Policy:

Default

Unique ID:

2. Fill in the data as shown:

- Logon ID - Using your Agency's domain (DOP in this case) slash (\) username (EX: DOP\warrenk)
- Password – enter your own. The initial password can be any generic password. The user will change it to his/her own hardened password at the first log in.
- Last Name and First Name.

- Click Save. Clicking on the “Save” button will create the UserID/Login ID. Once you’ve done this, you can manage this Login ID.

User created

Search

Search Criteria: User | All Data Sources | | Go | Advanced Search

Select All | Deselect All | Create User | Copy to New User | Delete | Unlock | Lock | Generate New Password | Export

| Type | Status | Logon ID | Name | Department | Data Source |
|------|--------|-------------|---------------|------------|-------------|
| | | DOP\warrenk | Kelly, Warren | | UME Databas |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Row 1 of 1

Details of User DOP\warrenk

Modify

General Information | Account Information | Contact Information | Additional Information | Assigned Roles | Assigned Groups | User Mapping for System Acc

Logon ID: DOP\warrenk

Last Name: Kelly

First Name: Warren

E-Mail Address:

Form of Address:

Language:

Activate Accessibility Feature: ☐

Security Policy: Default

Unique ID: USER.PRIVATE_DATASOURCE.un:DOP\warrenk

Assigning Group Roles to Professional LDAP or UME LogonID's

1. Search for a user using the [Advanced Search](#) described earlier, select it for editing.
2. Click on the Assigned Groups tab. You will see all the groups that are already assigned to the user. This will include default groups, and distribution lists.
3. Click on the Modify button to enter the edit mode.
4. Search for the Group to assign to the user in the Available Groups section. Enter the full name of the group or a part of the name with wildcards such as HR*
5. Click the Go button. This will show all the Available Groups that meet the search criteria (HR_HtmlGui_GRP in this example)

Available Portal GROUP Roles.

Portal BI Reporting GROUP Role:

- BI_REPORTS_GRP

Portal WEBGUI GROUP Role:

- HR_HtmlGui_GRP

Portal E-Recruiting Professional GROUP Roles:

- ER_Assessment_GRP
- ER_DecimalAdminLimited_GRP
- ER_DeCentralJSSupport_GRP
- ER_DecisionMaker_GRP
- ER_ManagerAsRecruiter_GRP
- ER_Recruiter_GRP
- ER_RecruiterLimited_GRP
- ER_RecruiterSupport_GRP
- ER_RequisitionRequest_GRP

Details of User WarrenK@DOP.WA.GOV

Save Cancel

General Information Account Information Contact Information Additional Information Assigned Roles Assigned Groups

Available Groups

Search Criteria All Data Sources ER Go

Select All Deselect All

| | Name | Description | Data Source |
|--------------------------|-------------------|----------------------|--------------|
| <input type="checkbox"/> | ER_DecimalAd... | Decentralized Adm... | UME Database |
| <input type="checkbox"/> | ER_DeCentralJS... | Job Seeker Suppo... | UME Database |
| <input type="checkbox"/> | ER_DecisionMa... | Decision Maker – ... | UME Database |
| <input type="checkbox"/> | ER_InternalCan... | My Career – ER G... | UME Database |
| <input type="checkbox"/> | ER_ManagerAs... | Manager as Recru... | UME Database |

Row 6 of 15

Add

Assigned Groups

Search Criteria All Data Sources ER*

Select All Deselect All

| | Name | Description | Data Source |
|--------------------------|--------------------|-----------------------|--------------|
| <input type="checkbox"/> | Everyone | Built-in Group Eve... | Built-in |
| <input type="checkbox"/> | G-S-HRISD STA... | Building1 and Buil... | LDAP |
| <input type="checkbox"/> | BI_Reports_GRP | DOP BI Reports G... | UME Database |
| <input type="checkbox"/> | Authenticated U... | Built-in Group Aut... | Built-in |

Row 1 of 4

Remove

Details of User WarrenK@DOP.WA.GOV

Save Cancel

General Information Account Information Contact Information Additional Information Assigned Roles Assigned Groups User Mapping

Available Groups

Search Criteria All Data Sources 4 5

Select All Deselect All

| | Name | Description | Data Source |
|--------------------------|----------------|---------------------|--------------|
| <input type="checkbox"/> | HR_HtmlGui_GRP | DOP HR WebGui Group | UME Database |

Row 1 of 1

Assigned Groups

Search Criteria All Data Sources

Select All Deselect All

| | Name | Description |
|--------------------------|-----------------------|--------------------|
| <input type="checkbox"/> | Everyone | Built-in Group Eve |
| <input type="checkbox"/> | G-S-Citrix Test Group | Group establish |
| <input type="checkbox"/> | G-S-HRISD STAFF | Building1 and Bu |
| <input type="checkbox"/> | G-S-HRMS Security | |
| <input type="checkbox"/> | BI_Reports_GRP | DOP BI Reports G |

Row 1 of 6

6. Click the box to the left of the Group name to select it. The row will be highlighted.
7. Click the Add button to add the Group role to the Assigned Groups section.

Details of User WarrenK@DOP.WA.GOV

Save Cancel

General Information Account Information Contact Information Additional Information Assigned Roles

Available Groups

Search Criteria All Data Sources

Select All Deselect All

| | Name | Description | Data Source |
|-------------------------------------|----------------|---------------------|--------------|
| <input checked="" type="checkbox"/> | HR_HtmlGui_GRP | DOP HR WebGui Group | UME Database |

Row 1 of 1

Assigned Groups

Search Criteria

Select All

| | Name | Description |
|--------------------------|------|-------------|
| <input type="checkbox"/> | Ev | |
| <input type="checkbox"/> | G- | |
| <input type="checkbox"/> | G- | |
| <input type="checkbox"/> | G- | |
| <input type="checkbox"/> | BL | |

8. Search and assign any additional Group roles if needed. Steps 4 - 7
9. Click the Save button to save the changes to the user account. The newly assigned Group Role(s) will be shown in the "Assigned Groups"
10. You will also need to user map the Portal account to the BI account. [Please refer to the Mapping to BI UserID.](#)

Details of User WarrenK@DOP.WA.GOV

Modify

General Information Account Information Contact Information Additional Information Assigne

Assigned Groups

Search Criteria All Data Sources Search Recursively Go

| Name | Description |
|-----------------------|----------------------------------|
| Everyone | Built-in Group Everyone |
| G-S-Citrix Test Group | Group established to test Citrix |
| HR_HtmlGui_GRP | DOP HR WebGui Group |
| G-S-HRISD STAFF | Building1 and Building5 Staff |
| G-S-HRMS Security | |

Assigning User Admin Single Role to Professional LDAP or UME LogonID's

1. Search for a user using the [Advanced Search](#) described earlier, select it for editing.
2. Click on the Assigned Roles tab.
3. Click on the Modify button to enter the edit mode.
4. Search for the User Admin role to assign to the user in the Available Roles section. Enter *User*Admin* in the criteria field
5. Click the Go button. This will show all the Available Roles that meet the search criteria (User Admin in this example). Choose the **User Admin** role.

Details of User WarrenK@DOP.WA.GOV

Save Cancel

General Information Account Information Contact Information Additional Information Assigned Roles Assigned Groups User Mapping for System Access

Available Roles

Search Criteria All Data Sources User* Go

Select All Deselect All

| Name | Description | Data Source |
|--------------------------|-------------|-------------|
| pcd:portal_content/ad... | User Admin | Portal Role |

Row 1 of 1

Add

Assigned Roles


Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

Row 0 of 0

Remove

6. Click the box to the left of the role name to select it. The row will be highlighted.
7. Click the Add button to add the User Admin role to the Assigned Roles section.
8. Click the Save button to save the changes to the user account. The User Admin Role will be shown in the "Assigned Roles". The message  User attributes modified will appear at the top of the screen.


Mapping to BI UserID

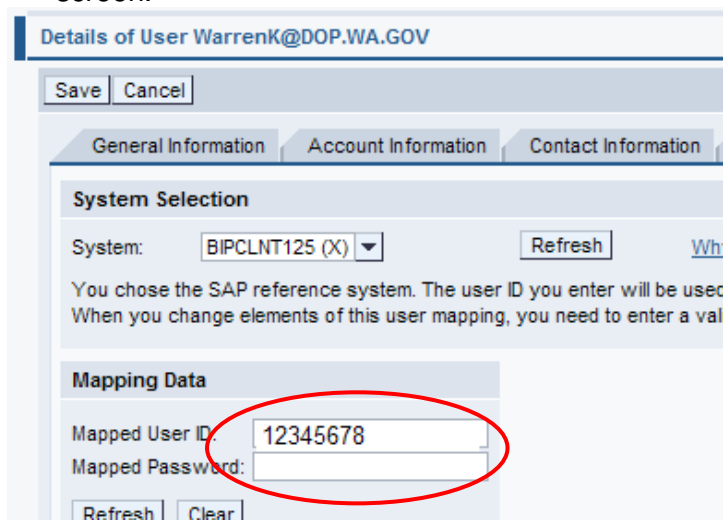
NOTE: The Professional Portal accounts need to be mapped to BI UserID accounts when the Professional Portal account has BI_Reports_GRP and/or HR_HtmlGui_GRP group or any E-Recruiting group role assigned.

***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapped to the Federated Portal. You will need to provide the BI UserID and current password and the Professional Portal account userID (LDAP or UME). Send requests to the DOP Service Center at servicecenter@dop.wa.gov or contact 360-664-6400.*

1. Search for a user using the [Advanced Search](#) described earlier, select it for editing.
2. Click on the User Mapping for System Access tab.
3. Click on the Modify button to enter the edit mode.
4. Enter the BIP UserID (8 digit personnel number including leading zeros) into the Mapped UserID field
5. Enter the BIP password for the UserID in the Mapped Password field

NOTE: You will have to know the user's BIP password. Most likely it will be the initial password that a BI User Admin created. If it is a productive password, BI User Admin should either reset it or ask the user for their productive BI password.

6. Click the Save button. The message  User attributes modified will appear at the top of the screen.



7. After a successful mapping you will see an X in the System drop down box BIPCLNT125 (X)



8. Remember to contact DOP to have the userid mapped in the Federated Portal!

Portal LogonID Maintenance

Reset Portal Logon ID Password

You can reset Portal user passwords in two cases:

- ESS users (8 digit personnel number)
- NON SSO professional users (domain\username)

NOTE: LDAP e-mail accounts' passwords are reset by your agency's Network Administrators this in turn will change the user's password to their PC.

NOTE: UME Professional and Personal ESS user account – if there is an email address in the email field of the account, the new initial password will be sent to the user after you reset it.

NOTE: When you are searching for an ESS User Portal account using the advanced search and no user comes up, try searching for their full 8-digit personnel number. The user might have changed their name, in that case you will have to update their name. If the user still does not come up in the search, contact the DOP Help Desk with the User's name and full 8-digit personnel number.

1. Search for a user that needs his/her password reset either using the search box, or the [Advanced Search](#) option.
2. Click on the box to the left of the user to select it, the line will become highlighted.

Welcome Julia Washburn Log Off HR

User Administration
Identity Management | Import | Activity Reports

Identity Management | History | Back Forward

Search

Search Criteria User All Data Sources dop* Go Advanced Search

Select All Deselect All Create User Copy to New User Delete Unlock Lock Generate New Password Export

| T... | Status | Logon ID | Name | Department | Data Source |
|-------------------------------------|--------|--------------|------------|------------|--------------|
| <input checked="" type="checkbox"/> | | dop\testuser | Test, User | | UME Database |

3. Click the Modify  Button to enter the edit mode.

Save Cancel

General Information Account Information Contact Information Additional Information Assigned Roles

Logon ID: * dop\testuser

☒ Define Initial Password
☐ Generate Password
☐ Disable Password

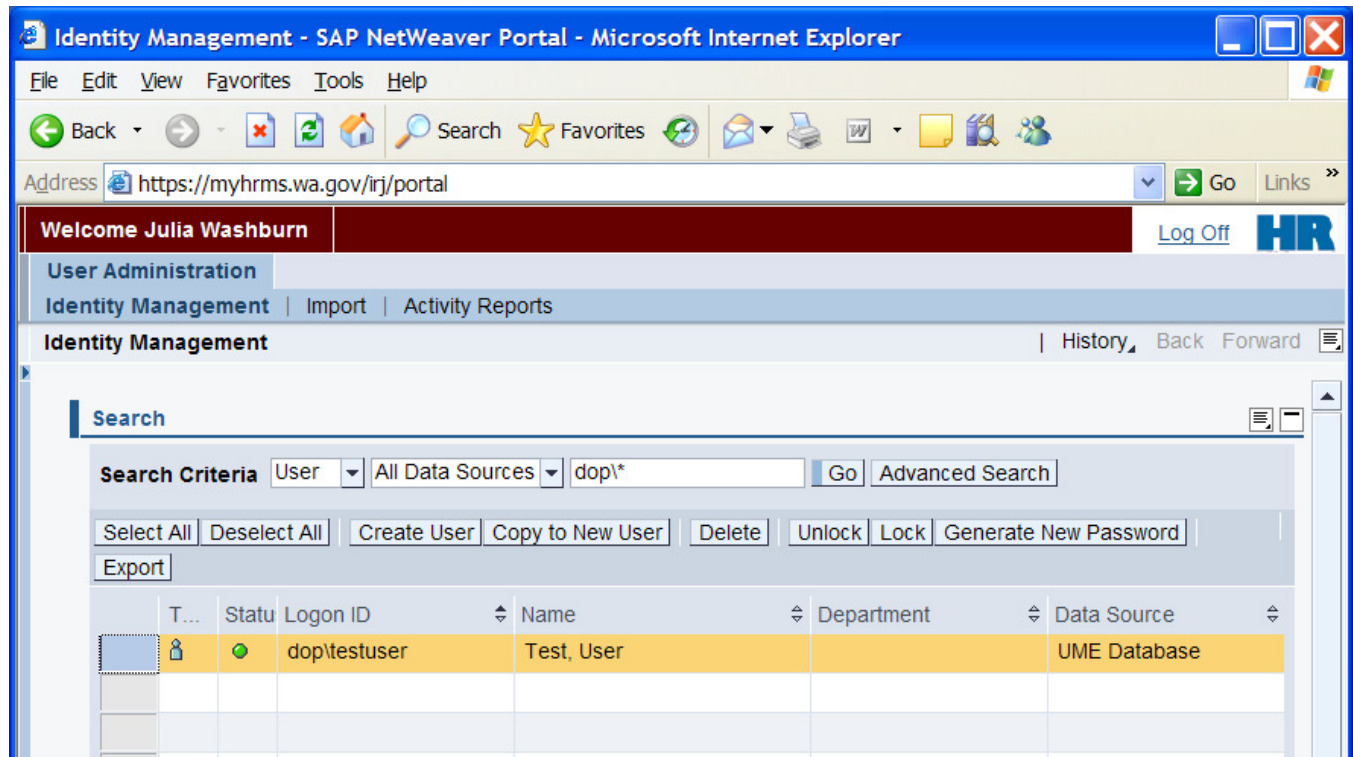
Define Password:
Confirm Password:

Last Name: * Test
First Name: User
E-Mail Address:

4. Enter Define Password and Confirm Password
5. Click the Save button

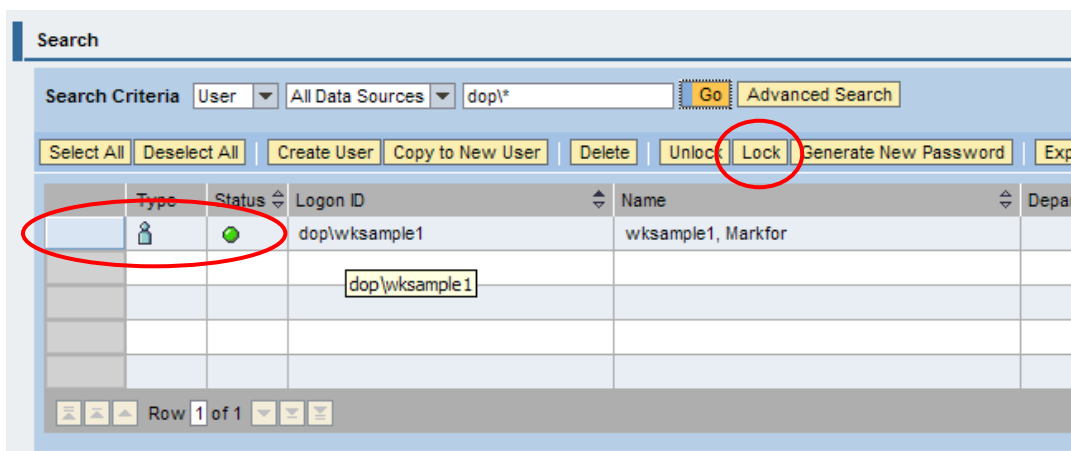
Lock/Unlock Portal Logon ID's

1. Logon to Portal; open your web browser and enter this URL: <https://myhrms.wa.gov/irj> or <https://wahrms.wa.gov/irj>.
2. Search for a user by either entering something in the search box (EX: dop*) or using the [Advanced Search](#) option.
3. Click the box to the left of the Logon ID to select the user.



To LOCK a specific Portal Logon ID

- a. At the search response form, click on the selection box to the left of the desired user's name and click the "lock" button



- b. You will be prompted to enter a reason for the lock, after entering reason text, click [Lock](#).

Search

Search Criteria User All Data Sources dopl* Go Advanced Search

Select All Deselect All Create User Copy to New User Delete Unlock Lock Generate New Password Export

You are locking user(s). Provide a reason for this action. This will be documented into each user's account history.

Message to Users:

Locking example 1

2nd Lock Cancel

| Type | Status | Logon ID | Name | Department |
|------|--------|---------------|--------------------|------------|
| | | doplwksample1 | wksample1, Markfor | |

- c. Upon successful lock, a message will appear and the user's Status Icon will change from Green Circle to a Blue Diamond.

User(s) locked

Search

Search Criteria User All Data Sources dopl* Go Advanced Search

Select All Deselect All Create User Copy to New User Delete Unlock Lock Generate New Password Export

| Type | Status | Logon ID | Name | Department |
|------|--------|---------------|--------------------|------------|
| | | doplwksample1 | wksample1, Markfor | |

Row 1 of 1

First row

To UNLOCK a specific Portal Logon ID

- d. Select the box to the left of the Portal Logon ID you want to unlock and click the Unlock button ABOVE the name.

The screenshot shows a 'Search' interface with a table of users. The 'Unlock' button in the toolbar is circled in red. The table has columns for Type, Status, Logon ID, Name, and Department. The first row shows a user with Logon ID 'dop\wksample1' and Name 'wksample1, Markfor'.

| Type | Status | Logon ID | Name | Department |
|------|--------|---------------|--------------------|------------|
| | | dop\wksample1 | wksample1, Markfor | |
| | | | | |
| | | | | |
| | | | | |

- e. You will be prompted to enter a reason for the unlock, after entering reason text, click the Unlock button BELOW the Reason box.

The screenshot shows a dialog box for unlocking a user. The 'Message to Users' text box contains 'UnLocking example 1'. The 'Unlock' button is circled in red. The background shows the same user table as the previous screenshot.

You are unlocking user(s). Provide a reason for this action. This will be documented in each user's account history.

Message to Users:

UnLocking example 1

1st

2nd

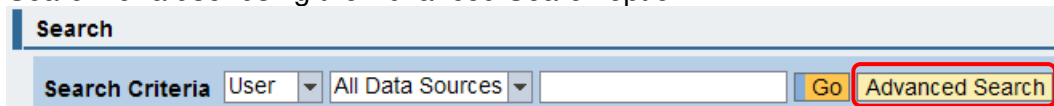
Unlock Cancel

- f. Upon successful unlock, a User(s) unlocked message will appear and the user's status icon will change to a green ball.

Delete PORTAL domain\username Accounts (UME)

NOTE: For the process when people leave your agency refer to [UserID Maintenance when Employees \(ESS/Professional Users\) Leave the Agency](#)

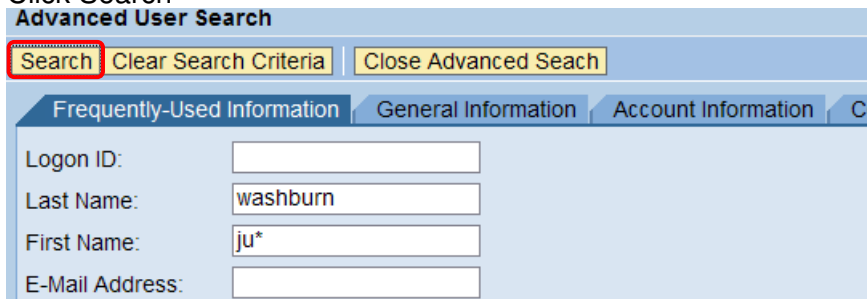
1. Logon to HRMS Portal; <https://myhrms.wa.gov/irj> or <https://wahrms.wa.gov/irj>.
2. Search for a user using the Advanced Search option.



Search

Search Criteria User All Data Sources Go Advanced Search

3. Enter Last Name and couple of letters of the first name with an *
4. Click Search



Advanced User Search

Search Clear Search Criteria Close Advanced Search

Frequently-Used Information General Information Account Information Contact Information

Logon ID:

Last Name: washburn

First Name: ju*

E-Mail Address:

5. Users will be displayed in the table.

- If your agency is outside the SGN your professional user accounts will be your agency domain\username such as **dop\username** (UME)
- If your agency is inside the SGN your professional user accounts will be your agency e-mail address such as LastFirst@dop.wa.gov (LDAP).
- 8 digit personnel number account could also be displayed. This is an ESS account.

Select All

Deselect All

Create User

Copy to New User

Delete

Unlock

Lock

Generate New Password

Export

| T... | ... | Logon ID | Name | Department | Data Source |
|------|-----|----------------------|-------------------------|------------|--------------|
| | | 00000000 | WASHBURN, JULIA | DOP | UME Database |
| | | dop\username | Washburn, Julia | | UME Database |
| | | LastFirst@dop.wa.gov | Washburn, Julia C (DOP) | | LDAP |

6. Click the box to the left of the Logon ID to select the user
7. Click the Modify button to enter the edit mode
8. Click the User Mapping for System Access
9. Click the Clear button to clear the mapping

****Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal. You will need to provide the BI UserID and current password and the Professional Portal account userID (LDAP or UME). Send requests to the DOP Service Center at servicecenter@dop.wa.gov or contact 360-664-6400.**

10. Click the Save button.

10

Save Cancel

Additional Information Customized Information Assigned Roles Assigned Groups **User Mapping for System Access** **8**

System Selection

System: SAP_BW (X) Refresh [Why are some systems missing?](#)

You chose the SAP reference system. The user ID you enter will be used for Single Sign-On to several or all SAP systems. When you change elements of this user mapping, you need to enter a valid password to prove your identity.

Mapping Data

Mapped User ID: 12345678

Mapped Password: **9**

Refresh Clear

11. With the user still selected click the “delete” button

Search

Search Criteria User All Data Sources dop* Go Advanced Search

Select All Deselect All Create User Copy to New User **Delete** Unlock Lock Generate New Password

Export

| T... | Statu | Logon ID | Name | Department | Data Source |
|----------|-------|--------------|------------|------------|--------------|
| 1 | ● | dop\testuser | Test, User | | UME Database |

12. Enter the reason for the account deletion and click Delete button.

The screenshot shows the Identity Management console interface. At the top, there is a search bar with the criteria 'User', 'All Data Sources', and 'dop*'. Below the search bar, there are several action buttons: 'Select All', 'Deselect All', 'Create User', 'Copy to New User', 'Delete', 'Unlock', 'Lock', 'Generate New Password', and 'Export'. The 'Delete' button is circled in red. Below the buttons, a confirmation message is displayed: 'Are you sure you want to delete selected user(s)? Provide a reason for this action. Message to Users:'. A text box contains the message 'Employee transferred to another agency.'. Below the text box, there are 'Delete' and 'Cancel' buttons. At the bottom, a table lists the users. The table has columns: 'T...', 'Statu', 'Logon ID', 'Name', 'Department', and 'Data Source'. The first row is highlighted in yellow and contains the following data: 'dop\testuser', 'Test, User', and 'UME Database'.

| T... | Statu | Logon ID | Name | Department | Data Source |
|------|-------|--------------|------------|------------|--------------|
| | | dop\testuser | Test, User | | UME Database |

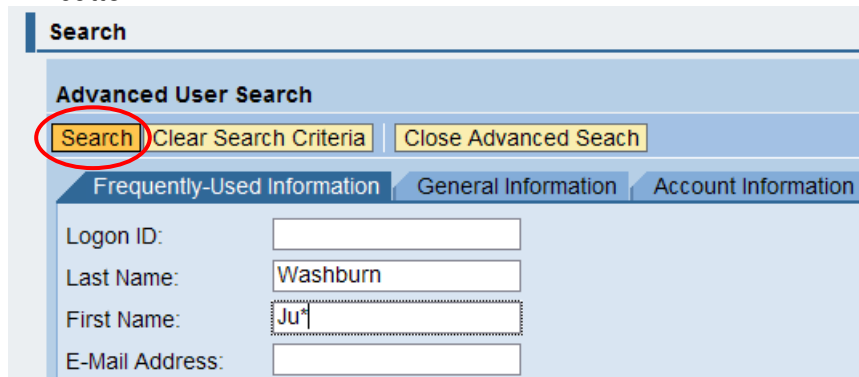
13. Upon successful deletion, the following message will appear at the top of the User List.

The selected user has been deleted or cleaned up

Delete Access from PORTAL E-Mail Account (LDAP)

NOTE: You cannot delete an LDAP e-mail account.

14. Logon to Portal; <https://myhrms.wa.gov/irj> or <https://wahrms.wa.gov/irj>.
15. Click the Advanced Search button
16. Enter the Last name and Couple of letters of the first name with an *, and click the Search button



Search

Advanced User Search

Search Clear Search Criteria Close Advanced Search

Frequently-Used Information General Information Account Information

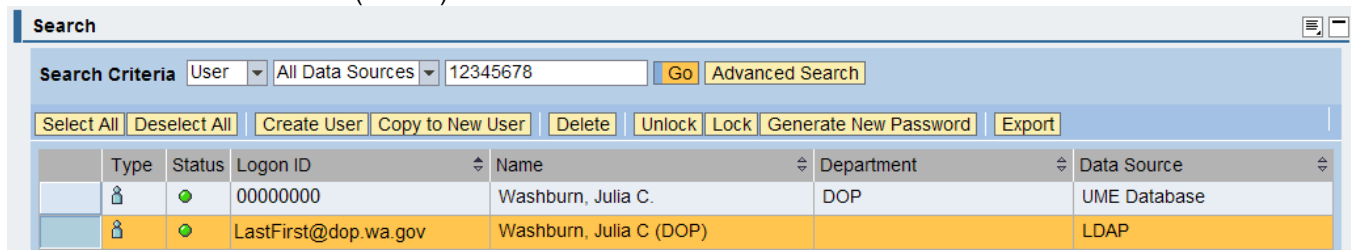
Logon ID:

Last Name:

First Name:

E-Mail Address:

17. Click on the e-mail (LDAP) account



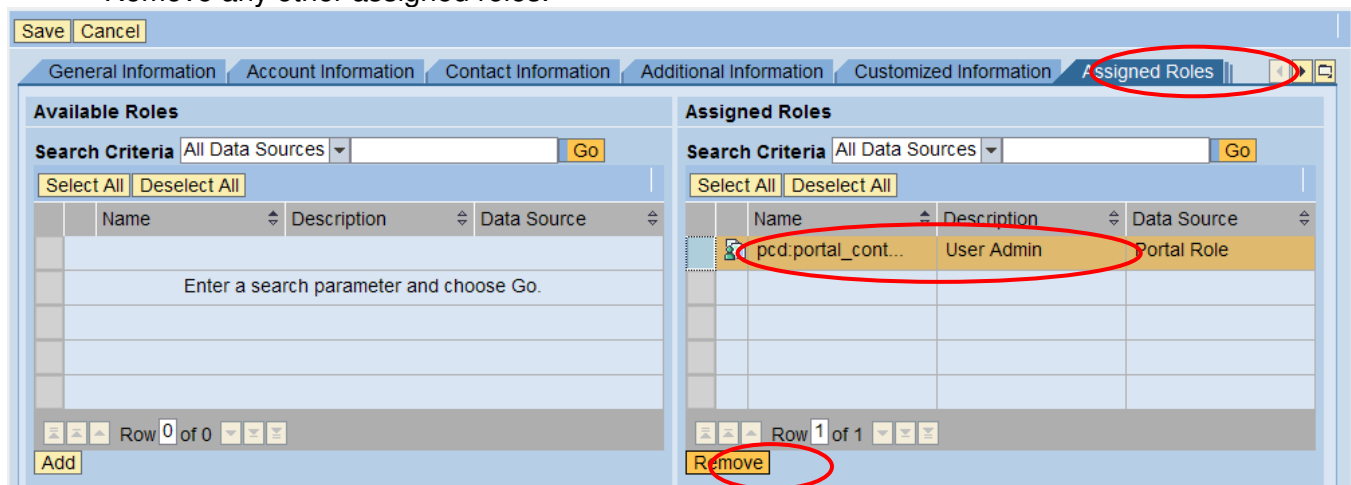
Search

Search Criteria User All Data Sources 12345678 Go Advanced Search

Select All Deselect All Create User Copy to New User Delete Unlock Lock Generate New Password Export

| Type | Status | Logon ID | Name | Department | Data Source |
|------|--------|----------------------|-------------------------|------------|--------------|
| | | 00000000 | Washburn, Julia C. | DOP | UME Database |
| | | LastFirst@dop.wa.gov | Washburn, Julia C (DOP) | | LDAP |

18. Click the Modify button to enter editing mode
19. Click the Assigned Roles tab. If there are any roles you need to delete them.
20. Click on the User Admin role
21. Click the Remove button; the removed role will be moved to the Available Roles section.
Remove any other assigned roles.



Save Cancel

General Information Account Information Contact Information Additional Information Customized Information **Assigned Roles**

Available Roles

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

Row 0 of 0

Add

Assigned Roles

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|--------------------|-------------|-------------|
| pcd:portal_cont... | User Admin | Portal Role |

Row 1 of 1

Remove

Save Cancel

General Information Account Information Contact Information Additional Information Customized Information Assigned Roles

Available Roles

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|--------------------|-------------|-------------|
| pcd:portal_cont... | User Admin | Portal Role |

Assigned Roles

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

22. Click on the Assigned Groups tab

23. Click on the All Data Sources drop down and choose UME Database and Click Go

Save Cancel

Contact Information Additional Information Customized Information Assigned Roles Assigned Groups

Available Groups

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

Assigned Groups

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|-------------------|----------------------|-------------------------|
| Everyone | | Built-in Groups Adapter |
| ER_Assessment... | Assessment – ER ... | UME Database |
| ER_DecisionMa... | Decision Maker – ... | UME Database |
| DOP DL ISD Pla... | | LDAP |
| DOP DL ISD Staff | | LDAP |

24. Click on the Group role

25. Click the Remove button; the removed Group Role(s) will be moved to the Available Groups section. Remove any remaining Group Roles.

Save Cancel

Contact Information Additional Information Customized Information Assigned Roles Assigned Groups

Available Groups

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

Assigned Groups

Search Criteria UME Database Go

Select All Deselect All

| Name | Description | Data Source |
|------------------|----------------------|--------------|
| Administrators | | UME Database |
| BI_Reports_GRP | DOP BI Reports G... | UME Database |
| ER_Assessment... | Assessment – ER ... | UME Database |
| ER_DecisionMa... | Decision Maker – ... | UME Database |

Add Remove

Save Cancel

Contact Information Additional Information Customized Information Assigned Roles Assigned Groups

Available Groups

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|------------------|----------------------|--------------|
| ER_DecisionMa... | Decision Maker – ... | UME Database |
| ER_Assessment... | Assessment – ER ... | UME Database |
| BI_Reports_GRP | DOP BI Reports G... | UME Database |

Assigned Groups

Search Criteria UME Database Go

Select All Deselect All

| Name | Description | Data Source |
|----------------|-------------|--------------|
| Administrators | | UME Database |

26. Click the User Mapping for System Access

27. Click the Clear button to clear the mapping

***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal. You will need to provide the BI UserID and current password and the Professional Portal account userID (LDAP or UME). Send requests to the DOP Service Center at servicecenter@dop.wa.gov or contact 360-664-6400.*

28. Click the Save button.

15

13

14

Additional Information | Customized Information | Assigned Roles | Assigned Groups | **User Mapping for System Access**

System Selection

System: SAP_BW (X) Refresh [Why are some systems missing?](#)

You chose the SAP reference system. The user ID you enter will be used for Single Sign-On to several or all SAP systems. When you change elements of this user mapping, you need to enter a valid password to prove your identity.

Mapping Data

Mapped User ID: 12345678

Mapped Password:

Refresh Clear

Non-Professional Users (ESS Users) Leave State Employment – Employee Status is Withdrawn:

HRMS PORTAL:

1. Logon to Portal; <https://myhrms.wa.gov/iri> or <https://wahrms.wa.gov/iri>
2. Search for a user by entering the 8 digit personnel number in the Search Box

3. Click on the Name of the User and click the Delete button

| T... | Status | Logon ID | Name | Department | Data Source |
|------|--------|----------|------------|------------|--------------|
| 1 | 1 | 12345678 | User, Test | | UME Database |

- Enter the reason for deletion and click the Delete button.

Search

Search Criteria: User | All Data Sources | 12345678 | Go | Advanced Search

Select All | Deselect All | Create User | Copy to New User | Delete | Unlock | Lock | Generate New Password | Export

Are you sure you want to delete selected user(s)? Provide a reason for this action.
 Message to Users:
 Employee is withdrawn

Delete | Cancel

| Ty... | Status | Logon ID | Name | Department | Data Source |
|-------|--------|----------|------------|------------|--------------|
| | | 12345678 | User, Test | | UME Database |

- After successful deletion, the following message will be displayed.

Search

Search Criteria: User | All Data Sources | 12345678

The selected user has been deleted or cleaned up

Professional Users Transfer out of the Agency or Professional Users Become Non-Professional Users (ESS Users):

HRMS PORTAL domain\username UME account:

- Logon to HRMS Portal; <https://myhrms.wa.gov/irj> or <https://wahrms.wa.gov/irj>.
- Search for a user using the Advanced Search option.

Search

Search Criteria: User | All Data Sources | | Go | **Advanced Search**

3. Enter Last Name and couple of letters of the first name with an *

4. Click Search

Advanced User Search

Search | Clear Search Criteria | Close Advanced Search

Frequently-Used Information | General Information | Account Information | Co

Logon ID: |

Last Name: washburn

First Name: ju*

E-Mail Address: |

- Users will be displayed in the table.
 - If your agency is outside the SGN your professional user accounts will be your agency domain\username such as **dom\username** (UME)

- If your agency is inside the SGN your professional user accounts will be your agency e-mail address such as LastFirst@dop.wa.gov (LDAP).
- 8 digit personnel number account could also be displayed. This is an ESS account.

Select All

Deselect All

Create User

Copy to New User

Delete

Unlock

Lock

Generate New Password

Export

| T... | ... | Logon ID | Name | Department | Data Source |
|------|-----|----------------------|-------------------------|------------|--------------|
| | | 00000000 | WASHBURN, JULIA | DOP | UME Database |
| | | dop\username | Washburn, Julia | | UME Database |
| | | LastFirst@dop.wa.gov | Washburn, Julia C (DOP) | | LDAP |

- Click the box to the left of the Logon ID to select the user and click the “delete” button

Search

Search Criteria: User | All Data Sources | dop* | Go | Advanced Search

Select All | Deselect All | Create User | Copy to New User | **Delete** | Unlock | Lock | Generate New Password | Export

| T... | Statu | Logon ID | Name | Department | Data Source |
|------|-------|--------------|------------|------------|--------------|
| | | dop\testuser | Test, User | | UME Database |

- Enter the reason for the account deletion and click Delete button.

Identity Management | History | Back | Forward

Search

Search Criteria: User | All Data Sources | dop* | Go | Advanced Search

Select All | Deselect All | Create User | Copy to New User | Delete | Unlock | Lock | Generate New Password | Export

Are you sure you want to delete selected user(s)? Provide a reason for this action.

Message to Users:

Employee transferred to another agency.

Delete | Cancel

| T... | Statu | Logon ID | Name | Department | Data Source |
|------|-------|--------------|------------|------------|--------------|
| | | dop\testuser | Test, User | | UME Database |

- Upon successful deletion, the following message will appear at the top of the User List.

The selected user has been deleted or cleaned up

HRMS PORTAL e-mail LDAP account:

NOTE: You cannot delete an LDAP e-mail account.

1. Logon to Portal; <https://myhrms.wa.gov/irj> or <https://wahrms.wa.gov/irj>.
2. Click the Advanced Search button
3. Enter the Last name and Couple of letters of the first name with an *, and click the Search button

Search

Advanced User Search

Search Clear Search Criteria Close Advanced Search

Frequently-Used Information General Information Account Information

Logon ID:

Last Name:

First Name:

E-Mail Address:

4. Click on the e-mail (LDAP) account

Search

Search Criteria User All Data Sources 12345678 Go Advanced Search

Select All Deselect All Create User Copy to New User Delete Unlock Lock Generate New Password Export

| Type | Status | Logon ID | Name | Department | Data Source |
|------|--------|----------------------|-------------------------|------------|--------------|
| | | 00000000 | Washburn, Julia C. | DOP | UME Database |
| | | LastFirst@dop.wa.gov | Washburn, Julia C (DOP) | | LDAP |

5. Click the Modify button to enter editing mode
6. Click the Assigned Roles tab. If there are any roles you need to delete them.
7. Click on the User Admin role
8. Click the Remove button; the removed role will be moved to the Available Roles section. Remove any other assigned roles.

Save Cancel

General Information Account Information Contact Information Additional Information Customized Information **Assigned Roles**

Available Roles

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

Row 0 of 0

Add

Assigned Roles

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|--------------------|-------------|-------------|
| pcd:portal_cont... | User Admin | Portal Role |

Row 1 of 1

Remove

Save Cancel

General Information Account Information Contact Information Additional Information Customized Information Assigned Roles

Available Roles

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|--------------------|-------------|-------------|
| pcd:portal_cont... | User Admin | Portal Role |

Assigned Roles

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

9. Click on the Assigned Groups tab

10. Click on the All Data Sources drop down and choose UME Database and Click Go

Save Cancel

Contact Information Additional Information Customized Information Assigned Roles Assigned Groups

Available Groups

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

Assigned Groups

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|-------------------|----------------------|-------------------------|
| Everyone | | Built-in Groups Adapter |
| ER_Assessment... | Assessment – ER ... | UME Database |
| ER_DecisionMa... | Decision Maker – ... | UME Database |
| DOP DL ISD Pla... | | LDAP |
| DOP DL ISD Staff | | LDAP |

11. Click on the Group role

12. Click the Remove button; the removed Group Role(s) will be moved to the Available Groups section. Remove any remaining Group Roles.

Save Cancel

Contact Information Additional Information Customized Information Assigned Roles Assigned Groups

Available Groups

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|---|-------------|-------------|
| Enter a search parameter and choose Go. | | |

Assigned Groups

Search Criteria UME Database Go

Select All Deselect All

| Name | Description | Data Source |
|------------------|----------------------|--------------|
| Administrators | | UME Database |
| BI_Reports_GRP | DOP BI Reports G... | UME Database |
| ER_Assessment... | Assessment – ER ... | UME Database |
| ER_DecisionMa... | Decision Maker – ... | UME Database |

Add Remove

Save Cancel

Contact Information Additional Information Customized Information Assigned Roles Assigned Groups

Available Groups

Search Criteria All Data Sources Go

Select All Deselect All

| Name | Description | Data Source |
|------------------|----------------------|--------------|
| ER_DecisionMa... | Decision Maker – ... | UME Database |
| ER_Assessment... | Assessment – ER ... | UME Database |
| BI_Reports_GRP | DOP BI Reports G... | UME Database |

Assigned Groups

Search Criteria UME Database Go

Select All Deselect All

| Name | Description | Data Source |
|----------------|-------------|--------------|
| Administrators | | UME Database |

13. Click the User Mapping for System Access

14. Click the Clear button to clear the mapping

***Effective April 26, 2010 you MUST also contact the DOP Service Center to have Professional Portal accounts mapping cleared from the Federated Portal. You will need to provide the BI UserID and current password and the Professional Portal account userID (LDAP or UME). Send requests to the DOP Service Center at servicecenter@dop.wa.gov or contact 360-664-6400.*

15. Click the Save button.

15

13

14

Save Cancel

Additional Information Customized Information Assigned Roles Assigned Groups **User Mapping for System Access**

System Selection

System: SAP_BW (X) Refresh Why are some systems missing?

You chose the SAP reference system. The user ID you enter will be used for Single Sign-On to several or all SAP systems. When you change elements of this user mapping, you need to enter a valid password to prove your identity.

Mapping Data

Mapped User ID: 12345678

Mapped Password:

Refresh Clear

Employee has a Name Change

NOTE: When an employee has a name change and the HCM personnel master record is updated, this change does not update the ESS User account (8 digit personnel number) or the UME professional account (domain/username) for that employee in the Portal. The Agency User Administrator must manually go into the Portal and change the employee's name on the ESS account, and recreate the Professional UME account with the new name and loginID.

Changing the Name in the ESS or domain\username (UME) Portal Account

1. Logon to Portal; <https://myhrms.wa.gov/irj> or <https://wahrms.wa.gov/irj>
2. Type in the user's 8digit personnel number in the search box for ESS user account

Search

Search Criteria User All Data Sources 00000000 Go Advanced Search

3. Click the Go **Go** button

Search

Search Criteria User All Data Sources 00000000 Go Advanced Search

Select All Deselect All Create User Copy to New User Delete Unlock Lock Generate New Password Export

| Type | Sta... | Logon ID | Name | Department | Data Source |
|------|--------|----------|-----------|------------|--------------|
| | | 00000000 | Doe, Jane | | UME Database |

4. Click on the user. The line will be highlighted in orange and the details will be displayed below

The screenshot shows a user management interface. At the top, there is a toolbar with buttons: Select All, Deselect All, Create User, Copy to New User, Delete, Unlock, Lock, Generate New Password, and Export. Below the toolbar is a table with columns: Type, Status, Logon ID, Name, Department, and Data Source. The first row is highlighted in orange and contains the following data: Type (User icon), Status (Green dot), Logon ID (00000000), Name (Doe, Jane), Department (), and Data Source (UME Database). Below the table is a pagination bar showing 'Row 1 of 1'. Below the table is a details pane titled 'Details of User 00000000'. The details pane has a 'Modify' button and several tabs: General Information, Account Information, Contact Information, Additional Information, Customized Information, and Assigned Roles. The 'General Information' tab is selected, showing fields for Logon ID (00000000), Last Name (Doe), First Name (Jane), and E-Mail Address ().

5. Click on the Modify **Modify** button

The screenshot shows the 'Details of User 00000000' pane in 'Modify' mode. At the top, there are 'Save' and 'Cancel' buttons. Below the buttons are several tabs: General Information, Account Information, Contact Information, Additional Information, Customized Information, and Assigned Roles. The 'General Information' tab is selected. The fields are as follows: Logon ID (00000000), Define Initial Password (selected), Generate Password (disabled), Disable Password (disabled), Define Password (), Confirm Password (), Last Name (Doe), First Name (Jane), and E-Mail Address ().

6. Edit the Last and/or First name

The screenshot shows a close-up of the 'Last Name' and 'First Name' fields. The 'Last Name' field is labeled 'Last Name: *' and contains the text 'Jackson'. The 'First Name' field is labeled 'First Name:' and contains the text 'Jane'. The 'E-Mail Address' field is partially visible below the first name field.

7. Click Save **Save**

Changing the LogonID for the domain\username (UME) Portal Account

NOTE: In order to change the LogonID in the UME Professional Portal account (domain\username) you will have to [create a new Professional Portal account](#) assign roles/group roles, and map to BI. Then delete the old Professional Portal account with the old name.